

COMPUTER NETWORK ACCEPTABLE USE

(This policy replaces existing Board of Education policy 5131.2–Computer and Internet Usage.)

The Board of Education is committed to optimizing student learning and teaching. The Board considers student and teacher access to a computer network, including the Internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in District classrooms for the purpose of advancing and promoting learning and teaching.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Brentwood School staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act.

The School Media Specialist, or designated representatives, will provide age appropriate training for students who use the District’s Internet facilities. The training provided will be designed to promote the District’s commitment to:

- a. The standards and acceptable use of Internet services as set forth in the District’s Internet Safety Policy;
- b. Student safety with regard to:
 - I. safety on the Internet;
 - II. appropriate behavior while on online, on social networking Web sites, and in chat rooms; and
 - III. cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children’s Internet Protection Act (CIPA)

The computer network can provide a forum for learning various software applications and, through online databases and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for students and staff.

All users of the District’s computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility.

- Users are not permitted to utilize the District’s technological resources to engage in any illegal or illicit behavior or behavior that violates any Board policy.
- Copyright laws must be followed.
- No one is permitted to deliberately damage any computer or computer-related equipment.
- No one is permitted to deliberately disrupt the operation of the network or its components, through the introduction of viruses or through other means.

COMPUTER NETWORK ACCEPTABLE USE

- Appropriate “netiquette” shall be followed at all times. **Students and staff should be aware that posting illegal, illicit or Board policy prohibited materials on the Internet that may foreseeably cause substantial disruptions to the school setting shall result in disciplinary measures.**
- **E-mail and other use of the District’s computer network are not private.**
- **Use of the District’s computers shall be solely for educational and business purposes.**

The Computer Network Acceptable Use Regulation (#4526-R) and Summary Flyer outlines in more detail the acceptable and unacceptable use and conduct while using the District’s computer network and accessing the Internet.

The Superintendent of Schools shall establish regulations governing the use and security of the District's computer network. All users of the District’s computer network and equipment shall comply with this policy and those regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating a computer network coordinator to oversee the use of District computer resources. The effective use of technology to support instruction requires the provisions of ongoing training. The District shall provide training to teachers in the use of educational technology and student data privacy. The Coordinator of Information Technology supervises and coordinates the District’s computer network. He/she or a member of his/her staff shall assist in providing training and updates to those staff using the District’s computer network.

With increased concern about identity theft, unwarranted invasion of privacy and the legal requirement under Education Law §2-d and its accompanying regulations to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Data Protection Officer. The Data Protection Officer will follow the regulations outlined in Policies 5500 and 8635 and their accompanying regulations and enter into contracts with all third-party vendors. If the third-party vendor refuses to enter into a contract with the district, the Coordinator of Information Technology may take action to prevent the use of the software/application from the third-party vendor, including the use of available technologies to block access from the district network.

Prior to any staff or student creating an online identity for the purpose of representing the district, one of the schools in the district or a district administered and sanctioned program, permission must be obtained from the Superintendent of Schools. Such online identities include domain names, social media accounts and video streaming channels. Upon approval, the Superintendent, or his/her designee working in conjunction with the Coordinator of Information Technology will facilitate the set-up of the online identity so that the district retains administrative ownership and control of the online identity.

The Superintendent, or his/her designee working in conjunction with the District’s Purchasing Agent, the Coordinator of Information and Technology shall hold the primary responsibility for

COMPUTER NETWORK ACCEPTABLE USE

the ordering of hardware and software for the instructional technology program. He/she shall prepare the yearly technology plan for New York State.

Cross-ref: 1800, Donations, Gifts, Grants to the District
4526.1, Internet Safety Policy
4526.1-R, Internet Safety Policy Regulation
4526-F, Student/Staff Attestation Form
5500, Student Records
5500-R, Student Records Regulation
5550, Student Privacy
8635, Information Security Breach and Notification
8635-R, Information Security Breach and Notification Regulation

Ref: Public Law No. 106-554
47 USC §254
20 USC §6801
N.Y Education Law §2-d
8 CRR-NY Part 121

Approved by the Board of Education:	02/13/07
Revision approved by the Board of Education:	08/21/08
Revision approved by the Board of Education:	01/19/17
Approved by the Board of Education:	06/18/20
Revision approved by the Board of Education:	01/19/23