Internet Acceptable Use: Filtering

6141.323.

Access to Electronic Networks:

Electronic networks, including the Internet, are a part of the district's instructional program in order to promote educational excellence by facilitating resource sharing, innovation and communication. In this policy and regulations hereunder, the computers, computer network, electronic devices, Internet access, and email system installed and provided by the Board are referred to collectively as the "electronic networks."

The Superintendent or his/her designee shall develop an administrative regulation containing an implementation plan for this policy. The implementation plan shall include, at a minimum, provisions for integration of the Internet in the curriculum, staff training, software filters and safety issues.

The district is not responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved or transmitted via the Internet. In addition, the district will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Acceptable Use, Privacy, and Monitoring:

The electronic network and computer systems are educational and business tools. All use of the district's electronic network must be:

1. in support of education and/or research and be in furtherance of the Board of Education's goals, or
2. for a legitimate school business purpose.

Use of the district's electronic networks is a privilege, not a right. The Board of Education reserves the right to monitor the use of the electronic networks to ensure they are being used in accordance with these regulations. **Users should have no expectation of privacy in the use of the electronic network or other electronic devices that access the electronic network. Use of the computer system represents an employee's acknowledgment that the employee has read and understands this policy and the applicable regulations in their entirety, including provisions regarding monitoring and review of computer activity.** General rules for behavior and communications apply when using electronic networks as contained in Board Administrative Policy, "Electronic Network Use" Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Notwithstanding the above and in accordance with state law, the Board may not: (1) request or require that an employee provide the Board with a user name and password, password, or any other authentication means for accessing a personal online account; (2) request or require that an employee authenticate or access a personal online account in the presence of the Board; or (3) require that an employee invite a supervisor employed by the Board or accept an invitation from a

supervisor employed by the Board to join a group affiliated with any personal online account of the employee. However, the Board may request or require that an employee provide the Board with a user name and password, password, or any other authentication means for accessing (1) any account or service provided by the Board or by virtue of the employee's employment relationship with the Baord or that the employee uses for the Board's business purposes, or (2) any electronic communications device supplied or paid for, in whole or in part, by the Board.

In accordance with applicable law, the Board maintains the right to require an employee to allow the Board to access his or her personal online account, without disclosing the user name and password, password, or other authentication means for accessing such personal online account, for the purpose of:

1. Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee's personal online account; or
2. Conducting an investigation based on the receipt of specific information about an employee's unauthorized transfer of the Board's proprietary information, confidential information, or financial data to or from a personal online account operated by an employee or other source.

For purposes of this policy, "personal online account" means any online account that is used by an employee exclusively for personal purposes and unrelated to any business purpose of the Board, including but not limited to electronic mail and retail-based Internet web sites. "Personal online account" does not include any account created, used, or accessed by an employee for purposes of the Board.

Curriculum:

The use of the District's electronic networks shall:

1. be consistent with the curriculum adopted by the Board of Education as well as the varied instructional needs, learning styles, abilities and developmental levels of the students, and
2. comply with the selection criteria for instructional materials and library media center materials.

Staff members may, consistent with the Superintendent's regulations and implementation plan, utilize the electronic networks throughout the curriculum for educational and legitimate school business purposes.

The district's electronic network is integral to the curriculum and is not a public forum for general use.

Internet Safety:

Each district computer with Internet access shall have a filtering device that blocks access to visual depictions that are obscene, pornographic or harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee. The Superintendent or his/her designee shall enforce the use of such filtering

devices. A principal or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or his/her designee.

District personnel shall educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, as well as cyber-bullying awareness and response, in conjunction with the Protecting Children in the 21st Century Act.

The Superintendent or his/her designee shall include measures in this policy's implementation plan and administrative regulation to address the following:

1. Restricting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including "hacking" and other unlawful activities; and
4. Limiting unauthorized disclosure, use and dissemination of personal identification information.

Authorization for Electronic Network Access:

Each student and his/her parent or guardian must sign the District's authorization form prior to being granted unsupervised use of the network.

All users of the District's electronic networks shall maintain the confidentiality of student records in accordance with state and federal law. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is placed onto the electronic networks.

The failure of any student or staff member to follow the terms of the authorization form, this policy or its accompanying administrative regulations will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Legal References:

Connecticut General Statutes:

1-210(b)(17) Access to public records. Exempt records.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

31-40x Employer inquiries re employee's or prospective employee's personal online accounts. Exceptions. Enforcement.

Federal law:

Family Educational Rights and Privacy Act of 1974, codified at 20 U.S.C. §§ 1232g *et. seq*.

34 C.F.R. 99.1-99.67

Children’s Internet Protection Act, Pub. L. No. 106-554, codified as amended at 20 U.S.C. § 7131

The Copyright Act of 1976, codified at17 U.S.C. 101 *et. seq.*

20 U.S.C. § 6318, as amended by Every Student Succeeds Act, Pub. L. No. 114-95 (2015)

FCC Order 03-188, July 23 2003

Cross Reference:

Policy 4034 (Employee Use of the District's Computer Systems and Electronic Communications

Policy 5500 (Student Use of the District's Computer Systems and Internet Safety)

Approved October 9, 2001

Amended March 23, 2004

Amended January 6, 2009

Amended December 6, 2016

Amended November 21, 2017

Previous Policy Number: HH1.3