Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use

Employees are to utilize the district's computers, networks, email system and Internet services for school-related purposes and performance of job duties. Limited incidental personal use of district computers, networks, email systems and Internet services is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations or other system users. "Limited incidental personal use" is defined as use by an individual employee for an appropriate, lawful, brief and occasional personal purposes. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

Employees shall be notified that computer files and electronic communications, including email and voice mail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or District operations without authority. The systems' security aspects, message delete function and personal passwords can be bypassed for monitoring purposes. Therefore, employees must be aware that they should not have any expectation of personal privacy in the use of these computer systems. This provision applies to any and all uses of the district's computer systems, including any incidental personal use permitted in accordance with this policy and applicable regulations.

Online/Internet Services

The Board will educate minor students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. Additionally, the Board will implement a technology protection measure to block or filter Internet access to visual depictions that are obscene material, contain child pornography, or are harmful to minors and ensure that such filtering technology is operative during computer use by minor students.

Any employee who violates this policy and/or any rules governing use of the district's computers will be subject to disciplinary action, up to and including discharge. Illegal uses of the school district's computers will also result in referral to law enforcement authorities.

All District computers remain under the control, custody and supervision of the school district. The school unit reserves the right to monitor all computer and Internet activity by employees. Employees have no expectation of privacy in their use of school computers.

NOTE: CABE recommends that local Boards require employees to sign an acknowledgment that they have read Board policy 4118.5/4218.5 and the regulations concerning computer use and include the following paragraph in the Board policy.

Each employee authorized to access the school district's computers, networks and Internet services is required to sign an acknowledgment form stating that they have read this policy and the accompanying regulations. The acknowledgment form will be retained in the employee's personnel file.

The Superintendent or his/her designee shall be responsible for overseeing the implementation of this policy and the accompanying rules and for advising the Board of the need for any future amendments or revisions to the policy/regulations. The Superintendent or his/her designee may develop additional administrative procedures/rules governing the day-to-day management and operations of the school district's computer system as long as they are consistent with the Board's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others as he/she deems appropriate.

Rules Concerning District-Sponsored Social Media Activity

1. In order for an employee to use social media sites as an educational tool or in relation to extracurricular activities or programs of the school district, the employee must seek and obtain the permission of his/her supervisor.

a. When permission is obtained, the employee and supervisor must complete and forward a Social Media Registry Form (Appendix A) to the Supervisor of Technology and the building principal.

2. If an employee wishes to use Facebook, Twitter, or other similar social media site to communicate meetings, activities, games, responsibilities, announcements etc., for a school-based club or a school-based activity or an official school-based organization, or an official sports team, the employee must also comply with the following rules:

a. The employee must set up the social media site and maintain sole control over the content including monitoring, etc. To the extent possible, the group list should be "closed" (e.g. membership in the group is limited to students, parents and appropriate school personnel, and "monitored" (e.g. the employee had the ability to access and supervise communications on the social media site).

b. To the greatest extent possible, members will not be established as "friends", but as members of the group list. When other social media sites are used, the employee will establish a similar parameter on the basis of the functionality of the social media site utilized.

c. Parents shall be permitted to access any page that their child has been invited to join.

d. Access to the page may only be permitted for educational purposes related to the club, activity, organization or team.

e. The employee responsible for the page will monitor it regularly.

f. The employee's supervisor shall be permitted access to any page established by the employee for a school-related purpose.

g. Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such district-sponsored social media activity.

3. Employees are required to refrain from making harassing, defamatory, obscene, abusive, discriminatory or threatening or similarly inappropriate statements in their social media communications on district-sponsored sites.

4. Employees are required to comply with all Board of Education policies and procedures and all applicable laws with respect to the use of computer equipment, networks or devices when accessing district-sponsored social media sites.

a. See Board of Education Policy 6141.322 for protocols and rules regarding display of student photos and student work on the Internet. All protocols and rules described in that policy apply to all Social Media publishing.

5. The Bristol Board of Education reserves the right to monitor all employee use of district computers and other electronic devices, including employee blogging and social networking activity. An employee should have no expectation of personal privacy in any communication made through social media while using district computers, cellular telephones or other data devices.

6. All communications through district-sponsored social media must comply with the Bristol Board of Education's policies concerning confidentiality, including the confidentiality of student information. If an employee is considering sharing information and is unsure about the confidential nature of the information, the employee shall consult with his/her supervisor prior to communicating such information.

7. An employee may not link a district-sponsored social media page to any personal social media sites or sites not sponsored by the school district.

8. An employee may not use district-sponsored social media communications for private financial gain, political, commercial, advertisement, and proselytizing or solicitation purposes.

9. An employee may not use district-sponsored social media communications in a manner that misrepresents personal views as those of the Board of Education, individual school or school district, or in a manner that could be construed as such.

Disciplinary Consequences

Violation of the Board's policy concerning the use of social media or these administrative regulations may lead to discipline up to and including the termination of employment consistent with state and federal law.

(cf. 6141.321 - Student Use of the Internet)

(cf. 6141.322 - Web Sites/Pages)

Legal References: Connecticut General Statutes

The Freedom of Information Act

31-48d Employers engaged in electronic monitoring required to give prior notice to employees. Exceptions. Civil penalty.

53a-182 Disorderly conduct; Class C misdemeanor

53a-182b Harassment in the first degree.

53a-183 Harassment in the second degree

53a-250 Computer-related Offenses: Definitions

Electronics Communication Privacy Act, 28 U.S.C. §2510 through 2520

Policy adopted: