

Personnel – Certified/Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

The Board of Education recognizes the importance and utility of social media and networks for its employees. The laws regarding social media continue to evolve and change. Nothing in this policy is intended to limit an employee's right to use social media under applicable law, as it may evolve. The Board acknowledges that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern. The Board will resolve any conflict between this policy and applicable law in favor of the law.

Ordinarily employee use of social media, including employees' personal use of social media, will not be a legal or policy issue. While a policy cannot address every instance of inappropriate social media use, employees must refrain from social media that:

1. interferes, disrupts, or undermines the effective operation of the school district;
2. is used to engage in harassing, defamatory, obscene, abuse, discriminatory or threatening, or similarly inappropriate communications to harass coworkers or other members of the school community;
3. creates a hostile work environment or learning environment;
4. breaches confidentiality obligations of school district employees, including, but not limited, to students' personally identifiable information, which is considered confidential in accordance with the Family Educational Rights and Privacy Act (FERPA);
5. disrupts the educational process;
6. uses social media to enter inappropriate contacts with students, their families, or guardians;
7. harms the goodwill and reputation of the school district in the community; or
8. violates the law, Board policies, and/or other school rules and regulations.

The Board of Education therefore adopts the following guidelines for the use of social media by Board of Education employees.

Personnel – Certified/Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Definitions:

- **Board of Education** includes all names, logos, buildings, images, and entities under the authority of the Board of Education.
- **Personally identifiable information** includes identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information, which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.
- **Social media** refers to online social interaction or other public display of personal information via electronic means and/or online tools and services that allow users to publish content and interact with their audiences. Current examples include the following websites or applications, including an employee's personal online account using such social media:
 - Social networking (e.g., Facebook, LinkedIn, Google+, Classmates.com);
 - Blogs and microblogs (e.g., Twitter, Tumblr, Medium);
 - Content-sharing (e.g., Scribd, SlideShare, DropBox);
 - Image-sharing, video-sharing, or livestreaming (e.g., Snapchat, Periscope, Flickr, YouTube, Instagram, Vine, Pinterest, TikTok);
 - Other sharing sites or applications such as by sound, location, news, or messaging, etc. (e.g., Reddit, Kik, WhatsApp, Facebook Messenger, WeChat).

Legal References:

U.S. Constitution, Amend I

Conn. Constitution, Article I, Sections 3, 4, 14

Conn. Gen. Stat. § 31-51q

Conn. Gen. Stat. § 53a-182; § 53a-183; § 53a-250

Family Educational Rights and Privacy Act Regulations, 34 CFR § 99.3

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

Personnel – Certified/Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning Personal Social Media Activity

1. An employee may not mention, discuss, or reference the Board of Education, the school district or its individual schools, programs, or teams on personal online social media accounts or other websites or applications, in a manner that could reasonably be construed as an official school district communication, unless the employee also states within the communication that such communication is the personal view of the employee of the school district and that the views expressed are the employee's alone and do not represent the views of the school district or the Board of Education. An example of such a disclaimer is: "the opinions and views expressed are those of the author and do not necessarily represent the position or opinion of the school district or Board of Education." An employee may "repost" or "share" online posts published by the Board of Education, the school district, or its individual schools related to school sponsored notifications, activities, team highlights, and scores without expressing a personal viewpoint or consistent with the above.
2. Employees are required to maintain appropriate professional boundaries with currently enrolled students, parents, and colleagues. For example, absent an unrelated relationship (e.g., relative, family friend, or personal friendship unrelated to school), it is not appropriate for an employee to "friend" a current student or his/her parent or guardian or otherwise establish special relationships with selected students through personal social media, and it is not appropriate for an employee to give students access to his/her personal posts unrelated to school.
3. Employees may not use the logo or trademarks of the Board of Education, school district or individual schools, programs, or teams of the school district on their personal posts, unless given written consent.
4. Employees are strongly recommended to use appropriate and respectful speech in their personal social media posts; and to refrain from harassing, defamatory, abusive, discriminatory, threatening, or other inappropriate communications. Such posts reflect poorly on the school district's reputation, can affect the educational process, and may substantially and materially interfere with an employee's ability to fulfill his/her professional responsibilities.

Personnel – Certified/Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning Personal Social Media Activity cont'd

5. Employees are individually responsible for their personal posts on social media. Employees may be sued by other employees, parents, or others that view an employee's social media posts as defamatory, pornographic, proprietary, harassing, libelous, or creating a hostile work or learning environment. In addition, employees should consider refraining from posting anything that belongs to another person or entity, such as copyrighted publications or trademarked images. As such activities are outside the scope of employment, employees may be personally liable for such claims.
6. Employees are required to comply with all Board of Education policies and procedures with respect to the use of district computer equipment, networks, or electronic devices when accessing social media sites. Any access to personal social media activities while on school property or using school district equipment is limited and must comply with those policies and may not interfere with an employee's duties at work. Employee personal use of social media during work hours should be limited to the employee's duty-free lunch time. Employees evaluated under the CCT Rubric for Effective Teaching understand the direct link between Domain 4: Professional Responsibilities and Teacher Leadership, and their personal social media use. Professional responsibility and ethics, positive school climate, and family and community engagement are part of Domain 4 and can be negatively affected by reckless activity on social media.
7. The Board of Education reserves the right to monitor all employee use of district computer equipment and/or electronic documents, data, and communications, including voice, e-mail, and Internet usage, including but not limited to, employee social media activity. An employee should have no expectation of personal privacy in any personal communication or post made through social media while using computers, cellphones, or other electronic data devices or network connections wireless or otherwise that are the property of the Board of Education, school district, or individual school.

Personnel – Certified/Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning Personal Social Media Activity cont'd

8. All posts on personal social media must comply with the Board of Education's policies concerning confidentiality, including but not limited to, the confidentiality of personally identifiable information and education records under FERPA. If an employee is unsure about the confidential nature of information the employee is considering posting, the employee shall consult with his/her supervisor prior to making the post.
9. An employee may not link a personal social media site or webpage to the Board of Education's website or the websites of the school district, individual schools, programs, or teams; or post material of the Board of Education, school district, individual schools, programs, or teams on a social media site or webpage without written permission of his/her supervisor unless in compliance with section 1 above.
10. All Board of Education policies that regulate off-duty conduct apply to social media activity including, but not limited to, policies related to public trust, illegal harassment, cyber-bullying, code of conduct, and protecting confidential information.

Access to Personal Online Accounts

1. An employee may not be required by his/her supervisor to provide his/her username, password, or other means of authentication of a personal online account.
2. An employee may not be required to authenticate or access a personal online account in the presence of his/her supervisor.
3. An employee may not be required to invite or accept an invitation from his/her supervisor or required to join a group with the employee's personal online account.

Notwithstanding, the Board of Education may require that an employee provide his/her username, password, or other means of accessing or authenticating a personal online account for purposes of accessing any account or service provided by the Board of Education for business purposes or any electronic communications device supplied by or paid for, in whole or in part, by the Board of Education.

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning District-Sponsored Social Media Activity

An employee who creates, manages, or posts for or on behalf of the Board of Education, school district or its individual schools, programs, or teams to a social media account is acting in an official capacity, and the following rules shall apply.

1. All social media accounts created by employees for or on behalf of the Board of Education, school district or its individual schools, programs, or teams remain the property of the Board of Education, school district, or its individual schools. The employee does not own such social media accounts. Account information, including passwords and e-mail addresses linked to a specific social media account, should be stored in a secured location that the employee's supervisor is aware of and has access to.
2. An employee who creates a social media account for or on behalf of the Board of Education, school district, or its individual schools, programs, or teams must use his/her school district e-mail address or other e-mail address designated by his/her supervisor and must refrain from using his/her personal e-mail address.
3. An employee must use strong passwords for social media accounts. Characteristics of a strong password include at least eight (8) characters, a mixture of both uppercase and lowercase letters, a mixture of letters and numbers, and inclusion of at least one special character (e.g., ! @ # \$?) when permitted.
4. An employee must set up multi-factor authentication on the account that is used to access the social media account. "Multi-factor authentication" is an electronic authentication method in which a user is required to successfully present two or more pieces of evidence (e.g., a pin code sent to the user's e-mail address) to be granted access to a website or application.
5. Use of social media accounts of the Board of Education, school district, or its individual schools, programs, or teams must be used for legitimate school and/or education related purposes and cannot be used for the employee's personal use.

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning District-Sponsored Social Media Activity cont'd

6. If an employee seeks to use social media websites or applications as an educational tool or in relation to extracurricular activities or programs of the school district or its individual schools, the employee must seek and obtain the written permission of his/her supervisor prior to creating the site.
7. If an employee wishes to use a social media site or application to communicate meetings, activities, games, responsibilities, announcements, etc., for a school-based club or a school-based activity or an official school-based organization, the employee must also comply with the following rules:
 - a. The employee must set up the account and/or group as a group list which will be “closed” (e.g., membership in the group is limited to students, parents, and appropriate school personnel) and “moderated” (e.g., the employee can access and supervise communications).
 - b. When Facebook is used as the social media site, members will not be established as “friends” but as members of the group list. When other social media sites or applications are used, the employee will establish a similar parameter based on functionality of the social media site or application utilized.
 - c. Anyone who has access to the communications conveyed through the site may only gain access by the permission of the employee (e.g., teacher, administrator, or supervisor). Persons desiring to access the page may join only after the employee invites them and allows them to join.
 - d. Parents and/or guardians shall be permitted to access any site that their child has been invited to join.
 - e. Access to a site may only be permitted for educational purposes related to the club, activity, organization, or team.
 - f. The employee responsible for the site will monitor it regularly.
 - g. The employee’s supervisor shall be permitted access to any site established by the employee for a school-related purpose.

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning District-Sponsored Social Media Activity cont'd

- h. Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such district-sponsored social media activity.
 - i. Names, profile images, and posts should all be clearly linked to the department or unit rather than the Board of Education, school district, or individual school.
- 8. Employees are required to use appropriate and respectful speech in their social media posts on district-sponsored sites; and to refrain from harassing, defamatory, abusive, discriminatory, threatening, or other inappropriate communications.
- 9. 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.
- 10. The Board of Education reserves the right to monitor all employee use of district computer equipment and/or district electronic devices, electronic documents, data, and communications, including voice, e-mail, and Internet usage, including social media activity. An employee should have no expectation of personal privacy in any communication or post made through social media while using computers, cellular telephones, or other electronic data devices or network connections wireless or otherwise that are the property of the Board of Education, school district, or individual school.
- 11. All posts on district-sponsored social media must comply with the Board of Education's policies concerning confidentiality, including the confidentiality of student information including but not limited to, personally identifiable information, which is considered confidential in accordance with the Family Educational Rights and Privacy Act (FERPA). If an employee is unsure about the confidential nature of information the employee is considering posting, the employee shall consult with his/her supervisor prior to making the post.
- 12. An employee may not link a district-sponsored social media site or webpage to any personal social media sites or sites not sponsored by the school district.

Personnel - Certified-Non-Certified

Rights, Responsibilities and Duties

Acceptable Computer Network Use (Employee Use of Technology)

Social Networking

Rules Concerning District-Sponsored Social Media Activity cont'd

13. An employee may not use district-sponsored social media communications for private financial gain, political, commercial, advertisement, proselytizing, or solicitation purposes. An employee may not use district-sponsored social media communications in a manner that misrepresents personal views as those of the Board of Education, school district or individual school, or in a manner that could be construed as such.

Disciplinary Consequences

Violation of this policy may lead to discipline up to and including the termination of employment consistent with state and federal law.

(cf. 4118.24/4218.24 – Staff/Student Non-Fraternization)

(cf. 4118.4/4218.4 – Electronic Mail)

(cf. 4118.5 – Acceptable Technology Use)

(cf. 4118.5/4218.5 – Acceptable Computer Network Use)

(cf. 4118.51_6141.325 – Use of New Web Tools (Blogging/Podcasting))

(cf. 4131 – Staff Development)

(cf. 5125 – Student Records, Confidentiality)

(cf. 6141.32 – Technology and Instruction)

(cf. 6141.321 – Responsible Student Computer, Network and Internet Use)

(cf. 6141.328 – Bring Your Own Device (BYOD) and Protocol for the Use of Technology in the Schools)

Legal Reference:

U.S. Constitution, Amend I

Conn. Constitution, Article I, Sections 3, 4, 14

Freedom of Information Act (FOIA)

Conn. Gen. Stat. § 31-40x

Conn. Gen. Stat. § 31-48d

Conn. Gen. Stat. § 31-51q

Conn. Gen. Stat. § 53a-182; § 53a-183; § 53a-250
Family Educational Rights and Privacy Act Regulations, 34 CFR § 99.3
Electronic Communication Privacy Act, 28 U.S.C. §§ 2510 through 2520

Policy adopted: October 14, 2021

STONINGTON PUBLIC SCHOOLS
Stonington, Connecticut