Social Media

Definitions

The rapid speed at which technology continuously evolves makes it difficult, if not impossible, to identify all types of social media.

Thus, the term **Social media** includes a variety of online tools and services that allow users to publish content and interact with their audiences. By way of example, social media includes the following websites or applications, including an employee's personal online account using such social media:

1. social networking (e.g. Facebook, LinkedIn, Google+, Classmates.com);
2. blogs and micro-blogs (e.g. Twitter, Tumblr, Medium);
3. content sharing (e.g. Scribd, SlideShare, DropBox);
4. image sharing, video sharing or live streaming (e.g. Snapchat, Periscope, Flickr, YouTube, Instagram, Vine, Pinterest, TikTok); and
5. other sharing site or apps such as by sound, location, news, or messaging, etc. (e.g. Reddit, Remind, Kik, Yik Yak, SoundCloud, WhatsApp).

Board of Education includes all names, logos, buildings, images, and entities under the authority of the Bethany Board of Education (Board).

Electronic communication devices include any electronic device that is capable of transmitting, accepting, or processing data, including, but not limited to, a computer, computer network and computer system, and a cellular or wireless telephone.

Personal online account includes 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, social media, and retail-based Internet websites. Personal online account does not include any account created, maintained, used, or accessed by an employee for a business, educational, or instructional purpose of the Board.

Rules Concerning District-Sponsored Social Media Activity

In order for an employee to use social media sites as an educational tool or in relation to extracurricular activities or programs of the Bethany Public School District (District), the employee must seek and obtain the prior permission of the IT Director and District administration.

Employees may not use personal online accounts to access social media for classroom activities without the express permission of the IT Director and District administration. Where appropriate and with permission, District-sponsored social media accounts should be used for such purposes.

If an employee wishes to use social media sites 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:

- The employee must receive the permission of the IT Director and District administration.
- The employee must not use his/her personal online account for such purpose but shall use his/her Board-issued account.
- The employee must ensure that such social media use is compliant with all Board of Education policies, regulations, and applicable state and federal law, including the provision of required legal notices and permission slips to parents.
- The employee must set up the club, etc. as a group list which will 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).
- Parents/guardians shall be permitted to access any page that their child has been invited to join.
- Access to the page may only be permitted for educational purposes related to the club, activity, organization, or team.
- The employee responsible for the page will monitor it regularly.
- The IT Director shall be permitted access to any page established by the employee for a school-related purpose.
- Employees are required to maintain appropriate professional boundaries in the establishment and maintenance of all such District-sponsored social media activity.

Employees are prohibited from making harassing, defamatory, obscene, abusive, discriminatory or threatening, or similarly inappropriate statements in their social media communications using District-sponsored sites or accounts or through Board-issued electronic accounts.

Employees are required to comply with all Board of Education policies and procedures and all applicable laws with respect to the use of electronic communications devices, networks, Board-issued accounts, or when accessing District-sponsored social media sites or while using personal devices on the District's wireless network or while accessing District servers.

The 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, including personal online accounts while using District electronic communication devices.

All communications through District-sponsored social media or Board-issued electronic accounts must comply with the 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 the District office prior to communicating such information.

An employee may not link a District-sponsored social media page to any personal online account or sites not sponsored by the District.

An employee may not use District-sponsored social media or Board-issued electronic accounts for communications for private financial gain, political, commercial, advertisement, proselytizing, or solicitation purposes.

An employee may not use District-sponsored social media or Board-issued electronic accounts in a manner that misrepresents personal views as those of the Board of Education or District, or in a manner that could be construed as such.

Rules Concerning Personal Online Accounts

The Board understands that employees utilize social media and the web for personal matters in the workplace. The Board reserves the right to monitor all employee use of District electronic communications devices, including a review of online and personal social media activities. An employee should have no expectation of personal privacy in any personal communication made through social media while using District computers, District-issued cellular telephones, or other electronic communications devices. While the Board reserves the right to monitor use of its electronic communications devices, employees may engage in incidental personal use of social media in the workplace so long as such use does not interfere with operations and productivity, and does not violate other Board policies.

An employee may not mention, discuss, reference, or link to the Board, the District or its individual schools, programs, or teams using personal online accounts or other sites or applications in a manner that could reasonably be construed as an official District communication, unless the employee also states within the communication that such communication is the personal view of the employee of the District and that the views expressed are the employee's alone and do not represent the views of the District or the Board. 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." For example, except as may be permitted by Board policy, employees may not provide job references for other individuals on social media that indicate that such references are made in an official capacity on behalf of the Board.

Employees are required to maintain appropriate professional boundaries with students, parents, and colleagues. For example, absent an unrelated online relationship (e.g., relative, family friend, or personal friendship unrelated to school), it is not appropriate for a teacher or administrator to "friend" a student or his/her parent or guardian or otherwise establish special relationships with selected students through personal online accounts, and it is not appropriate for an employee to give students or parents access to personal postings unrelated to school.

In accordance with the public trust doctrine, employees are advised to refrain from engaging in harassing, defamatory, obscene, abusive, discriminatory or threatening, or similarly inappropriate communications through personal online accounts. Such communications reflect poorly on the 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.

Employees are individually responsible for their personal communications through social media and other personal online accounts. Employees may be sued by other employees, parents or others, and any individual that views an employee's communication through social media and personal online accounts as defamatory, pornographic, proprietary, harassing, libelous, or creating a hostile work 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 all of these activities are outside the scope of employment, employees may be personally liable for such claims.

Employees are required to comply with all Board policies and procedures with respect to the use of electronic communication devices when accessing personal online accounts and/or social media through District computer systems. Any access to personal online accounts and/or personal social media activities while on school property or using District equipment must comply with those policies, and may not interfere with an employee's duties at work.

All communications through personal online accounts and/or social media must comply with the Board'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.

An employee may not post official Board material using a personal online account without written permission of the IT Director and District administration.

All of the Board's policies and Administrative Regulations apply to employee use of personal online accounts in the same way that they apply to conduct that occurs in the workplace and off-duty conduct.

Access to Personal Online Accounts

An employee may not be required by any District employee to provide his/her username, password, or other means of authentication of a personal online account.

An employee may not be required to authenticate or access a personal online account in the presence of any District employee.

An employee may not be required to invite or accept an invitation from any District employee or required to join a group with the employee's personal online account.

Use of Crowdfunding Activities

Prior to engaging in any crowdfunding activities (e.g. DonorsChoose, Kickstarter, GoFundMe, etc.) for the Board of Education, its school, classes, or extracurricular teams or clubs, an employee must first apply in writing to the Superintendent and receive approval for the crowdfunding activity. Such written application must include the name of the website or application to be utilized, a full description of the reason for the crowdfunding activity, a copy of the proposed personal profile to be listed on the site/application, and the proposed content to be uploaded to the crowdfunding website or application, including images. Any money received from crowdfunding activities must be deposited directly into a school fund and may not first be received by the employee. Crowdfunding activities must comply with all Board policies, Administrative Regulations, and procedures, and shall not include photos of students or the sharing of any confidential student information.

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.

An employee may face disciplinary action up to and including termination of employment if an employee transmits, without the Board's permission, confidential information to or from the employee's personal online account.

An employee may not be disciplined for failing to provide his/her username, password, or other authentication means for accessing a personal online account, failing to authenticate or access a personal online account in the presence of a District employee, or failing to invite a District employee or refusing to accept an invitation sent by a District employee to join a group affiliated with a personal online account, except as provided herein.

Notwithstanding, the Board 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 for business purposes or any electronic communications device supplied by or paid for, in whole or in part, by the Board.

Nothing in Board policy or this Administrative Regulation shall prevent the District from 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 an activity on an employee's personal online account or based on specific information about the transfer of confidential information to or from an employee's personal online account. During the course of such investigation, the District may require an employee to allow the District to access his/her personal online account for the purpose of conducting such investigation. However, the employee will not be required to provide his/her username and/or password or other authentication means in order for the District to access the personal online account.

Legal References: U.S. Constitution, Amendment I

Connecticut Constitution, Article I, §§ 3, 4, 14

Connecticut General Statutes § 31-40x

Connecticut General Statutes § 31-48d

Connecticut General Statutes § 31-51q

Connecticut General Statutes §§ 53a-182; 53a-183; 53a-250

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

Regulation approved: April 9, 2014
Regulation revised: October 6, 2016
Regulation revised: December 9, 2020

Source: Shipman