Book	Policy Manual
Section	800 Operations
Title	Social Media
Code	815.1
Status	Active
Adopted	May 12, 2015

Purpose

Both school district educational social media and commercial social media exist for Users to utilize. Therefore, social media could be used either as part of the school district's educational mission or for business purposes, or as part of the User's personal online presence with commercial social media. Mobile electronic devices, portable or stationary computers, and school district networks and systems, as well as Users' networks, systems, computers, and devices are available for (or provided for) Users to carry out their social media activities. The purpose of the Halifax Area School District ("school district" or "HASD") Social Media Policy is to establish rules and guidance for the use of social media by students, employees, and guests (collectively "Users").

A social media incident is a critical problem with the potential to injure students, employees, guests, and others, to lose confidential information and data, to set back any progress that the school district has previously made, to violate other's rights, and to subject the User or the school district to litigation.

Definitions

Guests - include, but are not limited to, visitors, workshop attendees, volunteers, adult education staff and students, school board members, independent contractors, vendors, and school district consultants.

Social Media[a] - includes websites that incorporate one (1) or more of the following:

Blogs – are web logs or journals where authors and users can post textual, audio, or video content, and where some permit others to post comments on their blogs. Some websites enable individuals to create free standing blogs, other special interest websites use blog tools and message forums to engage users.

Microblogs – are websites and spaces that allow users to post short blog entries. Twitter is an example, as well as other sites that invite users to post short status and location updates such as Foursquare and Schoology.

Social networks – are websites where users can create customized profiles and form connections with other users based on shared characteristics and interests. Websites such as Facebook and MySpace tend to foster personal social contact among "friends", while websites such as LinkedIn are oriented toward professional networking. Some school districts and businesses are also establishing a presence on social networks, for example with Schoology.

Media sharing – are websites where users post and share videos, audio files and/or photos as well as tag them to enable searchability. Examples include YouTube, Flickr, Picasa, and Google Video.

Wikis – are resources or documents edited collaboratively by a community of users with varying levels of editorial control by the website publisher. Wikipedia is an example.

Virtual worlds – Web or software-based platforms that allow users to create avatars or representations of themselves, and through these avatars to meet, socialize and transact with other users. Second Life and other virtual worlds are used for social purposes and e-commerce, non-profit fundraising, and videoconferencing.

Social media includes communication, collaborative sharing, and reaching students, employees and guests for educational purposes using school district provided websites, platforms, resources, or documents. Examples include but are not limited to: Google Apps, Ning, Flat Classroom, Teacher Tube, Moodle, YouTube, Ted, and Schoology.

Authority

The school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on and over *the school district's* CIS[b] systems and to monitor, record, check, track, log, access or otherwise inspect its CIS systems.[1]

In addition, *in accordance with the law (for example, relevant to this paragraph, with a search warrant, subpoena, court order, litigation procedure, or other legal means),* the school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored on User's personal computers, electronic devices, networks, Internet, electronic communication systems, and in databases, files, software, and media that contain school district information and data.

Also, *in accordance with the law (for example, relevant to this paragraph, with a search warrant, subpoena, court order, litigation procedure, or other legal means),* the school district has the right, but not the duty, to inspect, review, or retain electronic communication created, sent, displayed, received or stored *on another entity's* computer or electronic device when Users bring and use another entity's computer or electronic device to a school district location, event, or connect it to the school district network and/or systems, and/or that contains school district programs, or school district data or information.

The above applies no matter where the use occurs whether brought onto school district property, to school district events, or connected to the school district network, or when using mobile computing equipment and telecommunications facilities in protected and unprotected areas or environments, directly from home, or indirectly through another social media or Internet service provider, as well as by other means. All actions must be conducted in accordance with the law, assist in the protection of the school district's resources, ensure compliance with this policy, its administrative guidelines, or other school district policies, regulations, rules, and procedures, social media and Internet service providers terms, or local, state, and federal laws.

The school district will cooperate to the extent legally required with social media sites, Internet service providers, local, state, and federal officials in investigations or with other legal requests, whether criminal or civil actions.

Delegation of Responsibility

The school district intends to strictly facilitate a learning and teaching atmosphere, to foster the educational purpose and mission of the school district, and to protect its computers, devices, systems, network, information and data against outside and internal risks and vulnerabilities. Users are important and critical players in protecting these school district assets and in lessening the risks that can destroy these important and critical assets. Consequently, Users are required to fully comply with this Policy and its accompanying administrative guidelines, as well as the HASD's Acceptable

Use of Internet Policy #815 and all other relevant HASD policies, administrative guidelines, rules, procedures, social media terms of use and other legal documents, and local, state and federal laws. [2]

Users must immediately report any violations or suspicious activities to their principal or his/her designee, who in turn may contact the Director of Technology or his/her designee for assistance. The Director of Technology may be asked to, among others, assist in an investigation or to protect information or data. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this policy, and provided in other relevant school district policies and guidelines, rules and procedures. If a User believes there is a conflict in the requirements they are to comply with they must bring the matter to the attention of their supervisor, teacher, or administrator who will in turn assist the User.

It is the responsibility of all Users to carefully consider their behavior and what they place online when communicating with or "friending" any individual. The principal or designee, who in turn may contact the Director of Technology for assistance, is authorized to access Users' postings on public locations and on school district servers, hard drives, systems, and networks under the direction of the Superintendent, and/or designee, law enforcement, a court order, a subpoena or other legal action or authority. Users may not coerce others into providing passwords, login, or other security access information to them so that they may access social media or locations that they have no authorization to access. Users should note that information that they place in social media and designate as private can be accessed in litigation, can be distributed by their friends, and can be accessed in other various legal ways.

The Superintendent, and/or designee, is hereby granted the authority to create additional administrative guidelines, procedures, and rules to carry out the purpose of this Social Media Policy. The administrative guidelines, procedures, and rules accompanying this policy must include among other items guidance in implementing and using school district educational social media and commercial social media, and the responsibility of Users for their own behavior when communicating with social media.

Guidelines

It is often necessary to access Users' school district accounts in order to perform routine maintenance and for other legal reasons. System administrators have the right to access by interception, and to access the stored communication of User accounts for any reason in order to uphold this policy, accompanying administrative guidelines, the law, and to maintain the school district's system. **USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE SCHOOL DISTRICT'S CIS SYSTEMS, AND THE SCHOOL DISTRICT'S AUTHORIZED THIRD PARTIES' SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THESE SYSTEMS. The school district reserves the right to access, view, record, check, receive, monitor, track, log, store, and otherwise inspect and utilize any or all school district CIS systems, and authorized third parties' systems, and to monitor and allocate fileserver space. Users of the school district's CIS systems, and third party systems, who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications accessed, viewed, recorded, checked, received, monitored, tracked, logged, stored, and otherwise inspected or utilized by the school district, and to monitor and allocate fileserver space. Passwords and message delete functions do not restrict the school district's ability or right to access such communications or information.**

Users are responsible for their own behavior when communicating with social media. They will be held accountable for the content of the communications that they state/post on social media locations. Users are responsible for complying with the school district's employee, student, and guest conduct requirements. Users may not disrupt the learning atmosphere, educational programs, school activities, and the rights of others.

Inappropriate communications may not be included in Users social media, including but not limited to:

1. Confidential, personally identifiable, and sensitive school district information about students, employees, and guests;
2. Child pornography, sexual exploitation, bullying/cyberbullying, inappropriate commercialization of childhood experiences;
3. Defamatory or discriminatory statements and images;
4. Proprietary information of the school district and/or a school district's vendor;
5. Infringed upon intellectual property, such as copyright ownership, and circumvented technology protection measures;
6. Terroristic threats;
7. Unlawful threats against students, employees, and guests; and
8. Illegal items and activities.

Users may not use their personal computers, devices, services, systems, and networks to access social media sites during the time they are required to be fulfilling their work, learning, school responsibilities, or volunteer requirements unless they are permitted to do so by school district policy, administrative guideline, or an authorized employee, such as a teacher, principal, or Superintendent. The school district may block some social medial sites from use on its computers, devices, servers, networks, and systems; therefore, Users may not circumvent these technology protection measures to access the blocked, filtered, or unauthorized social media during their work, school, and volunteer responsibilities, unless approval has been granted by the Superintendent, and/or designee, and the commercial social media has been opened for that person(s) and purpose only.

Where Users place their communication in "privacy" marked social media, they cannot expect that their information will not be disclosed by a person within their "private marked group". Such information may be disclosed by others within the "private group", or the information may be discovered as part of the discovery process in litigation, or it may be disclosed by other means. The school district may be provided this information and be required to investigate it further. Information that the school district obtains may be disclosed without limitation for purposes of investigation, litigation, internal dispute resolution, and legitimate business purposes regardless of whether the particular User is involved.

Information that a User deleted may be recovered indefinitely by the school district.

The Superintendent or designee must provide training for employees and instructional sessions for students and, if appropriate, for guests to assist them in knowing the importance of and how to appropriately use social media, and how to comply with the requirements of this policy, and its accompanying administrative guideline(s), other relevant school district policies, guidelines, procedures and rules, website and Internet service provider terms, and local, state and federal laws. [3]

A User who has a material connection with the school district and endorses a school district product or service may have an obligation to disclose that relationship when the User makes such a statement using social media. The User should contact the Superintendent, and/or designee, to assess the various factors applicable in determining whether disclosure is applicable.[4]

Users may not use the name of the "Halifax Area School District" or its logo or mark in any form in social media, on school district Internet pages or websites, on websites not owned or related to the school district, or in forums/discussion boards, to express or imply the official position of the school

district without the expressed, written permission of the Superintendent, and/or designee. When such permission is granted, the posting must state that the statement does not represent the position of the school district.

Consequences for Inappropriate, Unauthorized and Illegal Use

General rules for behavior, ethics, and communications apply when using social networking systems and information, in addition to the stipulations of this Policy and its accompanying administrative guidelines. Users must be aware that violations of this Policy, accompanying administrative guidelines(s), or other school district policies, regulations, rules or procedures, or statutes, regulations and laws or unlawful use of social media systems and information, may result in loss of access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay for employees), dismissal, expulsions, breach of contract, penalties provided in statutes, regulations, and other laws and/or legal proceedings on a case-by-case basis. This policy, and its accompanying administrative guidelines, incorporate all other relevant school district policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, Digital Technology And Acceptable Use of Internet Policy, its accompanying administrative guidelines, and copyright, property, curriculum, terroristic threat, vendor access, harassment, and discrimination policies.[5][6][7][8][9]

a Social media can be engaged in by various ways, for example, through text messages, instant messages, and email by using personal accounts such as Gmail, Yahoo, and Hotmail on personally acquired services, systems, and networks, and/or through text messages, instant messages, and email by using school district accounts on school district services, systems, and networks. Personal digital assistants, cell phones, smartphones, computers, and other devices could be used to engage in social media. As well, chat services such as G-Chat, Blackberry Messenger, iChat, and FaceTime can be utilized. Additional social media may be developed in the future that could be covered by this Policy.

b "CIS" - computers, network, Internet, electronic communications, information systems, databases, files, software, and media.

Legal

1. 24 P.S. 510
2. Pol. 815
3. 47 U.S.C. 254
4. 16 CFR Part 255
5. 22 PA Code 235.2
6. 22 PA Code 235.4
7. 22 PA Code 235.5
8. 22 PA Code 235.10
9. 22 PA Code 235.11
22 PA Code 235.1 et seq

815.1-AR Social Media Acknowledge And Consent Form.docx (25 KB)

815.1-AR-1 Social Media Guidelines Employee Guests.doc (50 KB)

815.1-AR-2-Social Media Guidelines Students.docx (28 KB)