Employees Using Social Media to Represent the District

Issues to Consider Before Creating or Using a Professional Electronic Social Media Account

Before creating or using a professional electronic media site, a District employee must consider the following questions in determining whether the use of social media is appropriate:

- Who is the target audience for social media communications?
- What information is the school, district, group or individual attempting to communicate?
- Which social media tools are the best to distribute this information?
- Who is responsible for managing and monitoring the social media tools/accounts? Will this person represent the school or District appropriately?

Responsibilities

Employees should be thoughtful and professional about how they present the District, their school, school group, team or club, or individuals within schools or programs through the professional use of electronic social media sites. Employees must consider these issues:

- **Confidentiality**. Employees should not post or release proprietary, confidential, or protected personally identifiable information, or District intellectual property on professional electronic social media sites.
- **Privacy**. As in other venues, employees must follow the requirements of the Family Educational Rights and Privacy Act (FERPA) and must not post a student's image (including photos and/or video) or other protected personally identifiable information without ensuring the student's guardian has authorized the release of that information.
- **Site Monitoring**. Sites should be monitored for inappropriate posts or comments and follow the same guidelines as the school district's Social Media Rules of Engagement. Before removing inappropriate content, please contact the OSD Communications and Community Relations Department at 360-596-6103.

Creating and Administering Accounts

District employees wishing to create a professional electronic social media site representing the District, their school, school group, team or club, or individuals within schools or programs should first notify their school principal or department director and the district's Communications and Community Relations Office. The purpose of this notification is for District, school and department administrators to be aware of such sites and the communications taking place on these sites. The school or department administrator and the District's Communications and Community Relations Office shall be given administrative rights and/or passwords to the site at any time, upon request, in order to remove inappropriate posts or comments or otherwise make necessary changes to the site.

Best Practices to Mitigate Security Risks

When creating social media accounts that require individual identification, District employees must use their actual name, not pseudonyms. Employees should be mindful of these associated issues:

- Do not assume privacy. Only post information you are comfortable disclosing.
- Use different passwords for different accounts (such as social media and existing work accounts). Using the same password for all accounts increases the chance of the accounts being compromised.

- Do not duplicate user IDs and passwords across multiple social media sites.
- Use your school District e-mail to open social media sites rather than a private e-mail address.

Content of Posts and Comments

Professional electronic social media sites should be limited to instructional, educational, or extra-curricular activity matters. District employees should treat professional electronic media sites and communication like a classroom and professional workplace. The same standards of civility, decorum, and professional conduct that apply to District professional settings are expected on professional electronic social media site. Employees using social media to communicate on behalf of the District, a school, a school group, team or club, or individuals within schools or programs or themselves in their official District capacity should be mindful that any statements made are being made in their professional capacity.

Employees may not use professional electronic social networking sites for political purposes or to engage in private business activities. They should also refrain from posting statements, photographs, video or audio that could reasonably be perceived as:

- Sexually suggestive, malicious, obscene, profane, threatening or intimidating;
- Constituting harassment or bullying;
- Supportive of illegal activity;
- Violating copyright or trademark laws;
- Contributing to a hostile educational or work environment on the basis of race, religion, creed, color, national origin, age, honorably-discharged veteran, or military status, sex, sexual orientation, gender expression or identity, marital status, disability, or any other status protected by law; and/or
- Information that may tend to compromise the safety or security of the public or public systems.

Employees should always consider whether it is appropriate to post an opinion or discuss areas outside of one's expertise. If there is any question or hesitation regarding the content of a potential comment or post, the employee should not post. It is also not appropriate to engage in online arguments or use asocial media site to settle a disagreement with students, parents/guardians, staff, or community members.

The District reserves the right to restrict a District employee from using professional electronic media sites if they have violated this procedure or any applicable law. Employees may appeal this decision to the Superintendent or his/her designee. Employees should be mindful that inappropriate usage of social media may be grounds for disciplinary action.

Records Retention

Communications through professional electronic social media sites are public records and should be managed as such. All comments or posts made to professional electronic social media sites are public, not private. This means that all posts become part of the public record and may be subject to disclosure under Washington's Public Records Act (RCW 42.56). Social media account holders using professional electronic social media sites must retain those records to the extent required by law and adhere to the retention schedule set by the Washington State Archives.

Account administrators who receive messages through a private message service offered by the social media site should advise users to contact them at their District e-mail address. Private messages that account administrators receive should be treated as constituent e-mails and therefore, as public records. Account administrators or another authorized staff member should reply to such messages using their District e-mail account. Users should set all privacy settings to public.

Policy Adopted: January 5, 2015
Revised February 1, 2023