

All Personnel

EMPLOYEE USE OF TECHNOLOGY

Online/Internet Services: User Obligations and Responsibilities

Employees are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, guidelines, regulations, and the user obligations and responsibilities specified below.

1. The employee in whose name any account is issued is responsible for its proper use at all times. Employees shall keep account information, including logins and passwords, home addresses, and telephone numbers private. They shall use the system only under the login to which they have been assigned.
2. Employees shall use the system safely, responsibly, and primarily for work-related purposes. Use of district technology resources for personal purposes during break times or non-work may be allowed, but is subject to all the same policies and guidelines of other use. The employee's supervisor, or the Superintendent or designee, will have the right to determine if the personal use of such resources is excessive or interfering with the employee's work duties.
3. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

(cf. 4030 - Nondiscrimination in Employment)

(cf. 4031 - Complaints Concerning Discrimination in Employment)

(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)

5. Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.
6. Copyrighted material shall be posted online only in accordance with applicable copyright laws.

(cf. 6162.6 - Use of Copyrighted Materials)

7. Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.

EMPLOYEE USE OF TECHNOLOGY (continued)

8. Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the district or using district equipment or resources without permission of the Superintendent or designee. Such sites shall be subject to rules and guidelines established for district online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the district is not responsible for the content of the messages. The district retains the right to delete material on any such online communications.

The district may approve particular sites or systems for instructional, professional development, or communication purposes which are closed, moderated forums and designed to protect student safety. These sites include, but are not limited to social media, wiki's, blogs, and discussion forums.

9. Employees shall report any security problem or misuse of the services to the Superintendent or designee.

(cf. 1113 - District and School Web Sites)

Social Media

Employees shall exercise care when using any social media websites such as Facebook or MySpace, as well as Smart phones, text messaging and instant messaging, even when such use occurs in their own time using their own computer or device. Social media sites invite users to participate in informal ways that can leave the employee open to abuse, and often make little or no distinction between adult users and children.

Employees must maintain professional boundaries between themselves and all students. Employees should not allow any pupil to access personal information posted on a social media site. In particular, employees are advised to:

- Not add a pupil to a “Friends list” on their personal webpage.
- Ensure that personal information is not accessible via a “Public” setting, and ensure it is set to a “Friends only” level of visibility.
- Avoid contacting any pupil privately via a public social media website, text messaging and/or instant messaging services except for school related purposes when appropriate.
- Take steps to ensure that any person making contact via a social media website is who they claim to be, and not an imposter, before allowing them access to personal information.
- Not post pictures of students without parent permission.