USE OF SOCIAL MEDIA REGULATION

The District recognizes the prevalence of social media used for personal and educational purposes and acknowledges that American citizens have the right under the First Amendment to speak out on matters of public concern. However, it is essential that district patrons conduct themselves in such a way that their personal or educational use of social media does not adversely affect any other person (i.e. harassment, bullying, etc.). The purpose of this regulation is to outline expectations for social media use. Social media includes, but is not limited to: social networking websites such as MySpace, Facebook, Twitter, personal web pages or blogs, educational networking sites and electronic messaging.

Expectations for employee use of personal social media

- Refrain from accepting current students as "friends" on personal social networking sites.
- Be aware that people classified as "friends" have the ability to download and share your information with others.
- Remember that once something is posted to a social networking site it may remain available online even if you think it is removed and it may be far-reaching.
- Be aware of privacy settings and set appropriate levels of restriction.
- Not use a social networking site to discuss students or employees.
- Not post images that include students.

Expectations for student use of personal social media

- Be aware that people classified as "friends" have the ability to download and share your information with others.
- Remember that once something is posted to a social networking site it may remain available online even if you think it is removed and it may be far-reaching.
- *Set and maintain social networking privacy settings at the most restrictive level.*
- Not use a social networking site to bully, harass, or intimidate other students. Iowa Code 708.7 1.a(1)

Expectations for use of educational networking sites

District employees must:

- Notify your supervisor about the use of any educational network and discuss with your supervisor the need for notification to parents and other employees.
- Use District-supported networking tools when available.
- Be aware that all online communications are stored and can be monitored.
- Have a clear statement of purpose, conduct and outcomes for the use of the networking tool.
- Not post information about students, including images, names or other identifying information without parental release forms on file.

- Pay close attention to the site's security settings and allow only approved participants access to the site
- Follow all applicable copyright laws

District students must:

- Follow instructor's direction on purpose, conduct and outcomes for the use of the networking tool.
- Not post information about students, including images, names or other identifying information without instructor permission.
- Not use an educational networking site to bully, harass, or intimidate other students. Iowa Code 708.7 1.a(1)
- Follow all applicable copyright laws

Expectations for all networking sites

District employees should:

a) Not submit or post confidential or protected information about the District, its students, alumni or employees. Be aware that information about a student is protected from disclosure by both federal law(the Family Educational Rights and Privacy Act (FERPA) and state law (Iowa Code Section 22.7(1). Disclosures of confidential or protected information may result in liability for invasion of privacy or defamation.

b) Report, as required by law, any information found on a social networking site that falls under the mandatory reporting guidelines.

c) Not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.

d) Consider whether a particular posting puts your professional reputation and effectiveness as a District employee at risk.

e) Be cautious of security risks when using applications that work with the social networking site. (Examples of these sites are calendar programs and games.)

f) Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your personal computer.

g) Be alert to the possibility of phishing scams that arrive by email or on your social networking site.

h) All school e-mail communication for personal reasons should be on a limited basis. School email is subject to review and expected to meet the high standards of morality and ethics. (ITS #8)

(Revised 7/13/17)