Oskaloosa Community School District
Staff & Volunteer Technology Acceptable Use and Social Networking Policy

Computers are a powerful and valuable education and research tool and, as such, are an important part of the instructional program. In addition, the school district depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the board's expectations in regard to these different aspects of the school district's computer resources. Employees must conduct themselves in a manner that does not disrupt from or disrupt the educational process and failure to do so will result in discipline, up to and including, discharge.

General Provisions

The superintendent is responsible for designating a Technology Director who will oversee the use of school district computer resources. The school district will provide in-service programs for the training and development of school district staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

The superintendent, working with appropriate staff, shall establish regulations governing the use and security of the school district's computer resources. The school district will make every reasonable effort to maintain the security of the system. All users of the school district's computer resources, including students, staff and volunteers, shall comply with this policy and regulation, as well as others impacting the use of school equipment and facilities. Failure to comply may result in disciplinary action, up to and including discharge, as well as suspension and/or revocation of computer access privileges.

Usage of the school district's computer resources is a privilege, not a right, and that use entails responsibility. All information on the school district's computer system is considered a public record. Whether there is an exception to keep some narrow, specific content within the information confidential is determined on a case by case basis. Therefore, users of the school district's computer network must not expect, nor does the school district guarantee, privacy for e-mail or use of the school district's computer network including web sites visited. The school district reserves the right to access and view any material stored on school district equipment or any material used in conjunction with the school district's computer network.

The superintendent, working with the appropriate staff, shall establish procedures governing management of computer records in order to exercise appropriate control over computer records, including financial, personnel and student information. The procedures will address:

- passwords
- system administration
- separation of duties
- remote access
- data back-up (including archiving of e-mail)
- record retention
- disaster recovery plans

Social Networking or Other External Web Sites

For purposes of this policy any web site, other than the school district web site or school district sanctioned web sites, are considered external web sites. Social media networks are defined to include: web sites, blogs, wikis, social networks, online forums, and virtual worlds.

Employees shall not post confidential or proprietary information, including photographic images, about the school district, its employees, students, agents or others on any external web site without consent of their principal. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the school district when on external web sites.

Employees shall not use school district time, with the exception of lunch time, on external sites that are not in direct-relation to the employee's job.

Employees, students and volunteers need to realize that the Internet is not a closed system and anything posted on an external site may be viewed by others, all over the world. Employees, students and volunteers who don't want school administrators to know their personal information, should refrain from exposing it on the Internet.

Employees, who would like to use a social media network for school district sanctioned activities or classroom use, may do so, but must submit information about the social media site through the Social Media Networks form, and follow the Guidelines for Policy # 401.13: Social Media Networks.

Employees must avoid posting any information or engaging in communications that violate state or federal laws or District policies.

Employees are advised to maintain their professionalism as District employees and have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting. Because readers of social media networks may view the employee as a representative of the schools and the District, the District requires employees to observe the following rules when referring to the District, its schools, students, programs, activities, employees, volunteers and communities on any social media networks:

A. An employee's use of any social media network and an employee's postings, displays, or communications on any social media network must comply with all state and federal laws and any applicable District policies. (Student photos, privacy, confidentiality, etc.)

Employees must be respectful and professional in all communications (by word, image or other means). Employees shall not use obscene, profane or vulgar language on any social media network or engage in communications or conduct that is harassing, threatening, bullying, libelous, or defamatory or that discusses or encourages any illegal activity or the inappropriate use of alcohol, use of illegal drugs, sexual behavior, sexual harassment, or bullying.

Employees must make clear that any views expressed are the employee's alone and do not necessarily reflect the views of the District.

Employees may not act as a spokesperson for the District or post comments as a representative of the District, except as authorized by the Superintendent or the Superintendent's designee. When authorized as a spokesperson for the District, employees must disclose their employment relationship with the District.

Employees may not disclose information on any social media network that is confidential or proprietary to the District, its students, or employees or that is protected by data privacy laws.

Employees shall not use the school district logos, images, iconography, etc. on personal web sites that are not for school use.

Employees may not post images on any social media network of co-workers without the co-workers' consent.

Employees may not post images of students on any social media network without written parental consent, except for images of students taken in the public arena, such as at sporting events or fine arts public performances.

Employees may not post any building floor plans.

B. The District recognizes that student groups or members of the public may create social media representing students or groups within the District. When employees, including coaches/advisors, choose to join or engage with these social networking groups, they do so as an employee of the District. Employees have responsibility for maintaining appropriate employee-student relationships at all times and have responsibility for addressing inappropriate behavior or activity on these networks. This includes acting to protect the safety of minors online.

C. Employees who participate in social media networks may decide to include information about their work with the District as part of their personal profile, as it would relate to a typical social conversation. This may include:

1. Work information included in a personal profile, to include District name, job title, and job duties.
2. Status updates regarding an employee's own job promotion.
3. Personal participation in District-sponsored events, including volunteer activities.

D. An employee who is responsible for a social media network posting that fails to comply with the rules and guidelines set forth in this policy may be subject to discipline, up to and including termination. Employees will be held responsible for the disclosure, whether purposeful or inadvertent, of confidential or private information, information that violates the privacy rights or other rights of a third party, or the content of anything posted on any social media network.

E. Anything posted on an employee's web site or other Internet content for which the employee is responsible will be subject to all District policies, rules, regulations, and guidelines. The District is free to view and monitor an employee's web site at any time without consent or previous approval. Where applicable, employees may be asked to disclose to the District the existence of and to provide the District with access to an employee's web site or other personal social media network as part of an employment selection, promotion, or disciplinary process.

It is the responsibility of the superintendent to develop administrative regulations implementing this policy.

Legal Reference: Iowa Code § 279.8 (2011).
281 I.A.C. 13.35, .26

Cross Reference:
104 Anti-Bullying/Harassment
306 Administrator Code of Ethics
401.11 Employee Orientation
407 Licensed Employee Termination of Employment
413 Classified Employee Termination of Employment
605 Instructional Materials

Staff Technology Use Regulation

General

The following rules and regulations govern the use of the school district's computer network system, employee access to the Internet, and management of computerized records:

- Employees may be issued a school district e-mail account. Passwords must be changed periodically.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- Employees are expected to review their e-mail daily, and shall reply promptly to inquiries with information that the employee can reasonably be expected to provide.
- Communications with parents and/or students must be made with a school district email account, unless in the case of an emergency.
- Employees may access the Internet for education-related and/or work-related activities.
- Use of the school district computers and school e-mail address is a public record. Employees cannot have an expectation of privacy in the use of the school district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline, up to and including discharge.
- Use of the school district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Off-site access to the school district computer network will be determined by the superintendent in conjunction with appropriate personnel.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the school district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of school district computer use guidelines may be denied access to the school district's network.

Prohibited Activity and Uses

The following is a list of prohibited activity for all employees concerning use of the school district's computer network. Any violation of these prohibitions may result in discipline, up to and including discharge, or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising, or personal gain.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the school district computer network. *See Policy 605.7*, *Use of Information Resources* for more information.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material
- Using the network to receive, transmit or make available to others messages that are racist, sexist, and abusive or harassing to others.
- Use of another's account or password.
- Sharing passwords in an unsecure manner allowing others to gain access
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy school district equipment or materials, data of another user of the school district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

Other Technology Issues

Employees should contact students and their parents through the school district computer or phone unless in the case of an emergency or with prior consent of the principal. Employees should not release their cell phone number, personal e-mail address, etc. to students or their parents, except when overnight trips with students are involved. Employees, who are coaches or sponsors of activities, may create a text list of students and parents in order to communicate more effectively as long as the texts go to all students and the principal is included in the text address list. It is strongly recommended to use an online text messaging system, such as cel.ly that will keep records of all of the texts sent from the employee.

Oskaloosa Community School District
Guidelines for Policy #401.13: Social Media Networks

These are the guidelines for social media in the Oskaloosa School District. If you're an employee contributing to blogs, wikis, social networks, virtual worlds, or any other kind of social media both on and off the District network—these guidelines are for you. We expect all who participate in social media to understand and follow these guidelines. Failure to do so could put you at risk. These guidelines will continually evolve as new technologies and social networking tools emerge—so check back once in awhile to make sure you're up to date.

It's your responsibility. What you write is ultimately your responsibility. If it seems inappropriate, use caution. If you're about to publish something that makes you even the slightest bit uncomfortable, take time to review these guidelines. Ultimately, what you publish is your responsibility. What you publish is widely accessible and can be around for a long time, even after removing it from a site, so consider the content carefully. Trademark, copyright, and fair use requirements must be respected.

Ensure the safety of students. When employees, especially coaches/advisors, choose to join or engage with these social networking groups, they do so as an employee of the District and have responsibility for monitoring content and addressing inappropriate behavior or activity on these networks. This includes acting to protect the safety of minors online.

Be transparent. Your honesty—or dishonesty—will be quickly noticed in the social media environment. If you are posting about your work, use your real name and identify your employment relationship with the District. Be clear about your role; if you have a vested interest in something you are discussing, be the first to point it out. If you publish to a site outside the District's network, please use a disclaimer to state in clear terms that the views expressed are the employee's alone and that they do not necessarily reflect the views of the Oskaloosa School District.

Protect confidential information. Be thoughtful about what you publish. You must make sure you do not disclose or use confidential information. Students, parents, and colleagues should not be cited or obviously referenced without their approval. For example, ask permission before posting someone's picture in a social network (student photos require parental consent) or publishing a conversation that was meant to be private.

It is acceptable to discuss general details about projects, lessons, or events and to use nonidentifying pseudonyms for an individual (e.g., Teacher A) so long as the information provided does not make it easy for someone to identify the individual or violate any privacy laws. Furthermore, public social networking sites are not the place to conduct school business with students or parents.

Respect your audience and your coworkers. Always express ideas and opinions in a respectful manner. Make sure your communications are in good taste. Do not denigrate or insult others, including other schools or competitors. Remember that our communities reflect a diverse set of customs, values and points of view. Be respectful. This includes not only the obvious (no ethnic slurs, personal insults, obscenity, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory. Be sensitive about linking to content. Redirecting to another site may imply an endorsement of its content.

Perception can be reality. In online networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as a District employee, you are creating perceptions about your expertise and about the District by community members, parents, students, and the general public; and you are creating perceptions about yourself with your colleagues and managers. If you choose to join or engage with District students and families in a social media context, do so in a professional manner, ever mindful that in the minds of students, families, colleagues and the public, you are a District employee. Be sure that all content associated with you is consistent with your work and with the District's beliefs and professional standards.

Are you adding value? Communication associated with our District should help fellow educators, parents, students, and co-workers. It should be thought-provoking and build a sense of community. If it helps people improve knowledge or skills, do their jobs, solve problems, or understand education better—then it's adding value.

Keep your cool. One of the aims of social media is to create dialogue, and people will not always agree on an issue. When confronted with a difference of opinion, stay cool. If you make an error, be up front about your mistake and correct it quickly. Express your points in a clear, logical way. Don't pick fights, and correct mistakes when needed. Sometimes, it's best to ignore a comment and not give it credibility by acknowledging it with a response.

Be careful with personal information. Make full use of privacy settings. Know how to disable anonymous postings and use moderating tools on your social media site(s). Astute criminals can piece together information you provide on different sites and then use it to impersonate you or someone you know, or even re-set your passwords.

Be a positive role model. Educational employees have a responsibility to maintain appropriate employee-student relationships, whether on or off duty. Both case law and public expectations hold educational employees to a higher standard of conduct than the general public. You should make sure that your online activities do not interfere with your job. Remember that District technologies are provided for educational use. Use of social media for personal use during District time is prohibited.

Citing Sources: The published policies and guidelines of IBM, Intel and Kodak, and Minnetonka Public Schools, provided the foundation for Oskaloosa Community School District Employee Guidelines for social media, which were adapted for an educational organization.

*www.**minnetonka**.k12.mn.us/**policies/470.pdf***
http://www.kodak.com/US/images/en/corp/aboutKodak/onlineToday/Social_Media_9_8.pdf
http://www.intel.com/sites/sitewide/en_us/social-media.htm
http://www.ibm.com/blogs/zz/en/guidelines.html
Cyber Law: Maximizing Safety and Minimizing Risk in Classrooms; A. Bissonette, J.D. Corwin Press, 2009.

Oskaloosa Community School District
Staff & Volunteer Technology Acceptable Use and Social Networking Policy

I have read and understand the information provided about appropriate use of technology resources at the Oskaloosa Community School District. I agree to abide by these provisions and I understand that violations will have disciplinary actions and may lead to dismissal.

I understand that this form will be kept on file at the school.

_____
Employee name (print)

_____ Date _____
Employee signature

Building: ___ Elementary __ Middle School___ High School __ Webster

___ Bus Barn/Maint. Shop ___ Central Office

Position: ___ Teacher __ Assoc./Sec. ___ Nurse __ Admin/Director

___ Cust./Maint. __ Bus ___ Food Service __ Student Teacher

___ Substitute Teacher ___ Other

For Office Use Only:

Date Received: _____ Account Created: _____