

## Employees Acceptable Use Agreement

### BOARD POLICY:

The district will provide administrators, teachers, and other employees access to computers, networks, Internet, electronic mail (e-mail), and employee data systems through the district's internal and external Portal accounts. The purpose of this access is to promote educational excellence in schools by facilitating resource sharing, innovations, and communications. The use of computers, networks, the Internet, e-mail, and other online services shall be in support of education and research consistent with the educational objectives of the district.

#### Administrative Implemental Procedures:

1. **Services** The school district encourages employees to learn to use computers, networks, Internet, e-mail, and other online services and apply these tools in appropriate ways to the performance of tasks associated with their positions and assignments.
2. **Appropriate Use** Employees shall communicate with telecommunication tools in a professional manner consistent with state laws and district policies governing the behavior of school employees and with federal laws governing copyright. E-mail and telecommunications shall not be improperly utilized to disclose confidential information about district employees or to disclose information from student education records in violation of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, as amended, and its interpretive regulations, 34 C.F.R. § 99.1, *et seq.* This shall not apply to the student information system program or other district administrative software that is to be used by authorized employees in a manner that complies with FERPA and its interpretive regulations.
3. **Public Communication** Communication over networks should not be considered to be private. Messages may be diverted accidentally to another destination. The district network administrator(s) from time to time may review directories or messages to ascertain compliance with network guidelines for acceptable use. The network administrator(s) may delete files that are not kept to a manageable storage level or are deemed inappropriate.
4. **Student Access** Regardless of any "technology protection measure" implemented by the District as may be required by the Children's Internet Protection Act, teachers, administrators, and others who make decisions regarding student access to the Internet shall, in making such decisions, at all times consider the district's stated educational mission and the student acceptable use policy. To the extent possible, students' use of the Internet shall be structured in ways that point students to those resources that have been evaluated prior to use. District professional staff shall supervise students utilizing district-provided Internet access. Students shall not be allowed to utilize electronic communications unless a signed consent is on file. A family's right to decide whether or not to sign the Student Access Contract for their student shall be supported and respected. Permission is not transferable from one student to another and may not be shared.
5. **Violations** Employees who violate this policy will be subject to appropriate disciplinary action, up to and including termination.
6. **Inappropriate Use** The following uses of school-provided access to computers, networks, Internet, e-mail, and other online services are not permitted on the part of district employees:
  - a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material;
  - b. Transmitting obscene, abusive, sexually explicit, or threatening language;
  - c. Violating any local, state, or federal statute;
  - d. Accessing another employee's materials, information, or files without permission from the employee or the appropriate network administrator or principal;
  - e. Violating copyright or otherwise using the intellectual property of another individual or organization without permission;

- f. Using others' passwords and allowing students to use staff members' passwords;
- g. Vandalizing, which is any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses;
- h. Intentionally wasting limited resources;
- i. Using the network for commercial purposes;
- j. Harassing, insulting, or attacking others;
- k. Using e-mail lists from the district's Internet site, network, or servers to create mailing lists for non-school purposes;
- l. Gaining unauthorized access to resources or entities;
- m. Invading the privacy of individuals;
- n. Improperly altering the setup of computers (e.g., desktops, icons, wallpapers, screensavers, or installed software) as determined by the network administrator;
- o. Failing to follow district policies while using computers or failing to follow any other policies or guidelines established by district administration or the user's supervisor and failure to follow instructions of supervisors; and
- p. Seeking to gain or gaining unauthorized access to information resources or other computing devices.

**7. Security** Users are responsible for maintaining a safe, secure environment:

- a. Users will keep personal and district passwords secure; and
- b. Users will change passwords when directed by the network administrator.

**8. Security Risk** Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

**9. Copyright Law** shall be respected for all Internet and online services.

**10. Disclaimer** The district makes no warranties of any kind, whether express or implied, for the access it is providing, nor will it be responsible for any damages suffered. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at the user's risk. The district denies any responsibility for the accuracy or quality of information obtained through its system. The district is not liable for any commercial transactions conducted through its system.

**11. Statements of Personal Belief** Any statement of personal belief found on computers, networks, the Internet, e-mail, other on-line services, or any other telecommunication system shall be implicitly understood to be representative of the author's individual point of view, and not that of USD 345, its administrators, teachers, staff, or the participating school. No representations to the contrary shall be published without written approval from the designated district-level administrator(s). Principals, district-level administrators, or their designees may review all content in any Internet or on-line accounts paid for, in whole or in part, by the district or any school, without notice of any kind.

**12. Employee Acceptable Use Agreement and Annual Review**

- a. Prior to use of district computers, networks, the Internet, electronic mail, and other on-line services, the employee desiring to use such services shall submit a signed Employee Acceptable Use Agreement to the Building office for filing. An Employee Acceptable Use Agreement must be on file in order for the employee to have access to the above services, including an E-Mail account.
- b. Any employee who declines to sign an Employee Acceptable Use Agreement shall be denied access to the above services. In this event, the employee shall initial the Employee Acceptable Use Agreement to acknowledge awareness of this

Policy. The initialed Employee Acceptable Use Agreement shall be submitted to the Building office for filing.

- c. Each Building/School shall maintain a current list of employees who have signed Employee Acceptable Use Agreements and make it available to all principals, district office administrators, and their designees.
- d. School and district office administrators are required to meet with staff and review this Policy and any revisions prior to September 15 of each year. Administrators shall submit a signed statement to the District office verifying the completion of this annual review.
- e. This Policy applies to all employees regardless of whether or not they sign or initial an Employee Acceptable Use Agreement and/or attend annual review meetings related to this policy.

**13. District Technology Plan** The Administrative Implemental Procedures contained in this policy shall be consistent with the District Technology Plan adopted by the Board of Education.

**14. Document Retention Policy (DRP) Email Policy**  Thirty (30) days after being sent or received, Seaman USD will automatically delete any email in your email inbox, sent items and deleted items || folders that are not otherwise retained. Because some emails and associated attachments may be required to be maintained, for future reference, you may need to know how to create sub-folders in your email system to preserve those documents.

**15. Destroying Documents** After the district receives knowledge of legal action against the district or its employees, no documents or electronic information pertaining to the subject of the action, maintained in any form, may be destroyed.

**16. Damages** Certified employees will be provided one AC adapter (computer charger) upon employment with the district. Damage or loss of the AC adapter will result in a \$25 fee to cover replacement costs.

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_

### **Guidelines for the Use of Social Media**

Seaman recognizes that many staff, students, parents and community members are active on social media. As a school district, social media is also part of our communications strategy. These guidelines are designed to help you participate online in a respectful, relevant way that protects your reputation, the reputation of Seaman Schools, and that respects the relationship between teachers and students.

For the purposes of this document, social media includes, but is not limited to, social networking and media sharing sites such as Facebook, Twitter, Edmodo, Google+, LinkedIn, Instagram, Flickr, Tumblr, and YouTube. It also includes blogs, forums, web site comments, and any other activity online involving connecting or communicating with other users.

The first section of these guidelines cover general best practices. The second section addresses using social media as part of your job.

If you have additional questions, contact the USD 345 Director of Communications or call the Seaman Education Center.

#### **General Rules to Follow:**

Both case law and public expectations hold educational employees to a higher standard of conduct than the general public. **Be a positive role model and be aware of the image you present.**

**Online Is Forever** When you post something online, it is there forever and can be forwarded endlessly – thus becoming public and permanent. Deleting a post does not make it go away. Deleted content can still show up in online searches, or with the click of a button, other users can take a screen shot, re-post, or share your content with others. Even if you share content with a very limited number of people, nothing prohibits your contacts from sharing the information you post.

There have been many instances across the country of personal social media posts by employees of schools and government agencies becoming national news stories. Before you post or share content, ask yourself if you would want to see that content in the newspaper or on the evening news. **Would you feel comfortable if your content was read by colleagues, your students, parents, or the School Board?** If the answer is “no,” then the content is best not shared.

**Be mindful of your own safety and protect your privacy.** You are responsible for knowing the privacy settings on each social network you use. Always assume default settings will make your profile and any content you share publicly accessible. You should also understand that even with maximum privacy settings in place, content could still find its way in to the public domain.

**Perception can be reality** In online networks, the lines between public and private, personal and professional, are blurred. Simply by identifying yourself as working at Seaman you are creating perceptions about your expertise and the District. Be ever mindful that to patrons, you *are* a Seaman employee whether on the clock or not.

Many social media users include a prominent disclaimer saying they’re not speaking on behalf of their employer. This is good practice and is encouraged, but don’t count on it to avoid trouble.

**If you see abuse, you must report it** If you suspect abuse or neglect, you must report it. School personnel are mandatory reporters, in the real world and on the internet/social media.

**Identifying Students in Photos** *Do not identify or tag any elementary school student in photos posted online.* This is for student safety. It's fine if a parent tags or identifies a student in a photo you posted, but let them make that decision. Be aware that if a student is wearing a nametag, their name should be obscured in photos.

The only exception to not identifying elementary students is if the student is being featured in a news media story and is being identified by that venue.

Secondary students may be identified online unless a parent has presented an opt-out form to the school's office.

### **Interacting With Students And Parents On Social Media**

You have a responsibility to maintain appropriate employee-student relationships, whether on or off duty. ***Inappropriate relationships with students in a virtual environment could expose the employee to disciplinary action or termination.***

You are never under any obligation to accept friend or follower requests from any student or parent, or to use personal social media accounts to engage with students or participate in district projects. In addition, bear in mind that even if your account has privacy settings correctly configured, everything you post may be publicly accessible to your students and parents whether you are connected to them or not.

Employees must exercise great care in connecting with students on any social media channels. Do not send permission-based friend or follower requests to students, for example Facebook friend requests. If you decide to accept friend or follower requests from students you should accept all such requests, and not selectively limit interactions to what could be perceived as a few preferred individuals.

District employees might consider a statement such as the one that follows to include on their personal social media site(s): *If you are a parent or student requesting to be my Facebook friend, please do not be surprised or offended if I ignore your request. As an employee, practice discourages me from friending parents and students on my personal Facebook page.*

If you would like to connect with students or parents online, you are encouraged to set up a 'professional' account, as described in more detail below.

The district recognizes there may be certain limited exceptions to these guidelines, such as a student being a family member, or in instances where your interaction with a student is as a result of certain extra-curricular activities such as Boy Scouts, Girl Scouts, religious organizations, or other similar relationships.

### **Using Social Media Officially As Part Of Your Job**

**Ask yourself why** The first and most important step to take before you establish a social networking site for your classroom is to ask yourself several key questions:

- Why do you want to be engaged on a social media network?
- What information do you need to share, and is this the most effective platform on which to share the information?
- ***Do you have the time to maintain a social media page in a timely fashion?***

If you feel confident that your answers create a case for the use of social media, then you are ready to move forward.

**Develop Classroom Facebook sites as PAGES, not profiles (which are for personal use)** Facebook is a powerful tool for engaging stakeholders. However, your official page should be appropriately constructed. 'Pages' let you connect with students or parents while maintaining a clear boundary between your professional and personal life.

You may also decide to create an invitation-only Facebook group. Facebook groups are linked directly to your personal account, unlike Pages. However, they allow you to share information or photos with just members, whereas Pages are open to everyone. Remember, however, even in an invitation-only group, nothing stops members from sharing posts with the world.

Employees wishing to create and maintain a Facebook or other social media profile as a part of their job must contact the USD 345 Director of Communications.

**If you create it, you must monitor it** It is essential that if you determine a social media presence is an important part of your engagement strategy, you also make the commitment to monitoring comments as they are posted. Regular monitoring also enables you to respond in a timely manner to questions that are submitted.

Your posts and comments should help build and support the school community. You are responsible for what you post and communications that would be inappropriate or actionable if they occurred inside, or outside of the classroom do not become acceptable merely because they are made online. Always bear in mind that once posted, you cannot take it back.

**Social media should supplement, not replace, traditional classroom and parent communication.**

As pervasive as electronic devices are among students, be mindful that not all students have this form of access. Also, while most of our families have internet access, not all of them do, and not all parents use social media.

**Sources:**

Sources referenced in the development of these guidelines include: *University of Michigan, Ball State University, American Institute of Architects, Via Christi Health, Center for Technology in Government, Colorado State University, Sam Houston State University, United States Air Force, Guilford County Schools, Kodak, Kansas State University, Ohio State University Medical Center, Greteman Group, Minnetonka Public Schools, Wichita Public Schools, Eudora School District.*

Employee Signature: \_\_\_\_\_ Date: \_\_\_\_\_