Sheridan School District 48J

Code: **IIBGA-AR**
Revised/Reviewed: 12/15/10; 6/20/12; 12/17/14; 8/17/16
Orig. Code(s): IIBGA-AR

Electronic Communications System

Definitions

1. "Technology protection measure," as defined by the Children's Internet Protection Act (CIPA) means a specific technology that blocks or filters Internet access to visual depictions that are:

   a. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
   b. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
   c. Harmful to minors.

2. "Harmful to minors" as defined by CIPA means any picture, image, graphic image file or other visual depiction that:

   a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
   b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
   c. Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.

3. "Sexual act; sexual contact" as defined by CIPA have the meanings given such terms in Section 2246 of Title 18, United States Code.

4. "Minor" as defined by CIPA means an individual who has not attained the age of 17. For the purposes of Board policy and this administrative regulation, minor will include all students enrolled in district schools.

5. "Inappropriate matter" as defined by the district means material that is inconsistent with general public education purposes, the district's mission and goals.

6. "District proprietary information" is defined as any information created, produced or collected by district staff for the business or education purposes of the district including but not limited to student information, staff information, parent or patron information, curriculum, forms and like items used to conduct the district's business.

7. "District software" is defined as any commercial or staff developed software acquired using district resources.

General District Responsibilities

The district will:

1. Designate staff, or appropriate services (e.g., ESDs, contracted services), as necessary to ensure coordination and maintenance of the district's electronic communications system which includes all district computers, e-mail and Internet access;

2. Provide staff training in the appropriate use of the district's system including copies of district policy and administrative regulations. Staff will provide similar training to authorized system users;

3. Provide a system for authorizing staff use of personal electronic devices to download or access district proprietary information, that insures the protections of said information and insures its removal from the device when its use is no longer authorized;

4. Provide a system for obtaining prior written agreement from staff for the recovery of district proprietary information downloaded to staff personal electronic devices as necessary to accomplish district purposes, obligations or duties, and when the use on the personal electronic device is no longer authorized, to insure verification that information downloaded has been properly removed from the personal electronic device;

5. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district's system;

6. Use only properly licensed software, audio or video media purchased by the district or approved for use by the district. The district will comply with the requirements of law regarding the use, reproduction and distribution of copyrighted works and with applicable provisions of use or license agreements;

7. Install and use desktop and/or server virus detection and removal software;

8. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to the use of computers by minors, harmful to minors. An administrator, supervisor or other individual authorized by the superintendent may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;

9. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web;

10. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including "hacking" and other unlawful activities online, and ensure the safety and security of minors when authorized to use e-mail, chat rooms and other forms of direct electronic communication;

11. Provide student education about appropriate online behavior, including cyberbullying awareness and response; and how to interact with other individuals on social networking and social media websites and in chat rooms;

12. Determine which users and sites accessible as part of the district's system are most applicable to the curricular needs of the district and may restrict user access, accordingly;

13. Determine which users will be provided access to the district's e-mail system;

14. Notify appropriate system users that:

    a. The district retains ownership and control of its computers, hardware, software and data at all times. All communications and stored information transmitted, received or contained in the district's information system are the district's property and are to be used for authorized purposes only. Use of district equipment or software for unauthorized purposes is strictly prohibited. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the district's system are in compliance with Board policy, administrative regulations and law, school administrators may routinely review user files and communications.
    b. Files and other information, including e-mail, sent or received, generated or stored on district servers are not private and may be subject to monitoring. By using the district's system, individuals consent to have that use monitored by authorized district personnel. The district reserves the right to access and disclose, as appropriate, all information and data contained on district computers and district-owned e-mail system;
    c. The district may establish a retention schedule for the removal of e-mail;
    d. E-mail sent or received by a Board member or employee in connection with the transaction of public business may be a public record and subject to state archivist rules for retention and destruction;
    e. Information and data entered or stored on the district's computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the district. "Deleted" or "purged" data from district computers or e-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the district;
    f. The district may set quotas for system disk usage. The district may allow system users to increase their quota by submitting a written request to the supervising teacher or system coordinator stating the need for the increase;
    g. Passwords used on the district's system are the property of the district and must be provided to their supervisor or designated district personnel, as appropriate. Passwords that have not been provided to the district are prohibited;
    h. Transmission of any materials regarding political campaigns is prohibited.
    i. For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time.
    j. The district reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
    k. Postings by employees from a district email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the district, unless posting is in the course of business duties.
    l. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

15. Ensure all student, staff and nonschool system users complete and sign an agreement to abide by the district's electronic communications policy and administrative regulations. All such agreements will be maintained on file in the school office.

16. Notify users of known copyright infringing activities and deny access to or remove the material.

17. A log will be kept that records the sites visited when accessing the Internet. The district reserves the right to search these logs when there are allegations of misuse or concern about sites being visited.

18. The district will archive email for up to one year.

19. The district will keep logs of Internet usage for up to one month.

System Access

1. Access to the district's system is authorized to:

   Board members, district employees, students in grades K-12, with parent approval and when under the direct supervision of staff, and district volunteers, district contractors or other members of the public as authorized by the system coordinator or district administrators consistent with the district's policy governing use of district equipment and materials.

2. Students, staff and Board members may be permitted to use the district's system to conduct business related to the management or instructional needs of the district or to conduct research related to education. Personal use of district computers including Internet and e-mail access by students and Board members is strictly prohibited. Personal use of district computers including Internet access and e-mail by staff is restricted. Any personal use by staff is limited to such uses as deemed permissible under the Oregon Government Ethics Commission (OGEC) guidance (e.g., occasional use to type a social letter to a friend or family member, preparation of application materials for another position in the district, or computer games which may serve to improve the individual's keyboard proficiency and software component familiarity). Such use is restricted to the employee's own time.

General Use Prohibitions/Guidelines/Etiquette

Operation of the district's system relies upon the proper conduct and appropriate use of system users. Students, staff and others granted system access are responsible for adhering to the following prohibitions and guidelines which require legal, ethical and efficient utilization of the district's system.

1. Prohibitions

   The following conduct is strictly prohibited:

   a. Attempts to use the district's system for:
      (1) Unauthorized solicitation of funds;
      (2) Distribution of chain letters;
      (3) Unauthorized sale or purchase of merchandise and services;

(4) Collection of signatures;
(5) Membership drives;
(6) Transmission of any materials regarding political campaigns.

b. Attempts to upload, download, use, reproduce or distribute information, data or software on the district's system in violation of copyright law or applicable provisions of use or license agreements;
c. Attempts to degrade, disrupt or vandalize the district's equipment, software, materials or data or those of any other user of the district's system or any of the agencies or other networks connected to the district's system;
d. Attempts to evade, change or exceed resource quotas or disk usage quotas;
e. Attempts to send, intentionally access or download any text file or picture or engage in any communication that includes material which may be interpreted as:

(1) Harmful to minors;
(2) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district;
(3) A product or service not permitted to minors by law;
(4) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others;
(5) A likelihood that, either because of its content or the manner of distribution, it will cause a material or substantial disruption of the proper and orderly operation of the school or school activity;
(6) Defamatory, libelous, reckless or maliciously false, potentially giving rise to civil liability, constituting or promoting discrimination, a criminal offense or otherwise violates any law, rule, regulation, Board policy and/or administrative regulation.

f. Attempts to gain unauthorized access to any service via the district's system which has a cost involved or attempts to incur other types of costs without specific approval. The user accessing such services will be responsible for these costs;
g. Attempts to post or publish personal student contact information unless authorized by the system coordinator or teacher and consistent with applicable Board policy pertaining to student directory information and personally identifiable information. Personal contact information includes photograph, age, home, school, work or e-mail addresses or phone numbers or other unauthorized disclosure, use and dissemination of personal information regarding students;
h. Attempts to arrange student meetings with anyone on the district's system, unless authorized by the system coordinator or teacher and with prior parent approval;
i. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
j. Attempts to use another individual's account name or password, fail to provide the district with individual passwords or to access restricted information, resources or networks to which the user has not been given access;
k. Connecting wirelessly or directly to the district's network with non-district owned devices, including but not limited to, laptop or desktop computers; PDA's (e.g., iPads, Dell Axim, etc.); iPods; iPhones; Smart phones; network packet sniffing equipment; wireless access points; hubs; routers; and switches. Such devices will be immediately disconnected and removed upon discovery and the network port disabled pending further action;

l. Unauthorized copying of copyrighted material included, but not limited to, digitization and distribution of photographs from magazines; books or other copyrighted sources; copyrighted music; and the installation of any copyrighted software for which the district or the end user does not have an active license is strictly prohibited;
m. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The IT department should be consulted prior to export of any material that is in question;
n. Using a district computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;
o. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet;
p. Providing information about, or lists of, district employees to parties outside the district without authorization of the district.

2. Guidelines/Etiquette

System users will:

a. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and administrative regulations;
b. Respect other people's time and cyberspace. Use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher or system coordinator. Avoid downloading excessively large files. Remain on the system long enough to get needed information then exit the system. Act as though every byte sent costs somebody time and money, because it does;
c. Take pride in communications. Check spelling and grammar;
d. Respect the privacy of others. Do not read the mail or files of others without their permission;
e. Cite all quotes, references and sources;
f. Adhere to guidelines for managing and composing effective e-mail messages:

(1) One subject per message - avoid covering various issues in a single e-mail message;
(2) Use a descriptive heading;
(3) Be concise - keep message short and to the point;
(4) Write short sentences;
(5) Use bulleted lists to break up complicated text;
(6) Conclude message with actions required and target dates;
(7) Remove e-mail in accordance with established guidelines;
(8) Remember, there is no expected right to privacy when using e-mail. Others may read or access mail;
(9) Always sign messages;
(10) Always acknowledge receipt of a document or file.

g. Protect password confidentiality. Passwords are the property of the district and are not to be shared with others. Using another user's account or password or allowing such access by another may be permitted with supervising teacher or system coordinator approval only. No

system user may use a password on the district's computers, e-mail system or Internet access which is unknown to the district;

h. Communicate only with such users and/or sites as may be authorized by the district;
i. Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques;
j. Report violations of the district's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate;
k. If you are planning leave or vacation and another employee, or temporary employee, will fill in for you, contact the district office prior to being out of the office. The employee fulfilling your role will be issued appropriate email, voicemail and network action for use during the time you are gone. Do not give this individual your login and/or password information. If this is to be an extended leave, i.e., 10 days or more, an account is to be created for the temporary employee, rather than granting access to your account. Your email and other functions on the network can be forwarded or transferred to this employee so that they may function in your role as a replacement as necessary.

Complaints

Complaints regarding use of the district's Electronic Communications System may be made to the teacher, principal, employee's supervisor or system coordinator. The district's established complaint procedure will be used for complaints concerning violations of the district's Electronic Communications System policy and/or administrative regulation. See Board policy KL - Public Complaints and accompanying administrative regulation.

Violations/Consequences

1. Students

    a. Students who violate general system user prohibitions shall be subject to discipline up to and including expulsion and/or revocation of district system access up to and including permanent loss of privileges.
    b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
    c. Disciplinary action may be appealed by parents, students and/or a representative in accordance with established district procedures.

2. Staff

    a. Staff who violate general system user prohibitions shall be subject to discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements and applicable provisions of law.
    b. Violations of law will be reported to law enforcement officials and may result in criminal or civil sanctions.
    c. Violations of applicable Teacher Standards and Practices Commission (TSPC), Standards for Competent and Ethical Performance of Oregon Educators will be reported to TSPC as provided by Oregon Administrative Rule (OAR) 584-020-0041.
    d. Violations of Oregon Revised Statute (ORS) 244.040 will be reported to OGEC.

3. Others

    a. Other guest users who violate general system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
    b. Violations of law will be reported to law enforcement officials or other agencies, as appropriate, and may result in criminal or civil sanctions.

Telephone/Membership/E-mail/Other Charges

1. The district assumes no responsibility or liability for any membership or phone charges including, but not limited to, long distance charges, per minute (unit) surcharges and/or equipment or line costs incurred by any home usage of the district's system.

2. Any disputes or problems regarding phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider.

3. Telephone voicemail inboxes will be provided to district staff as a means for employees of the district, other staff, and outside parties – such as parents, to communicate with those who are assigned inboxes.

4. E-mail shall be considered an appropriate mechanism for official communication by the district with the employees of the district unless otherwise prohibited by law. The district reserves the right to send official communications to employees by e-mail with the full expectation that employees will receive e-mail and read these e-mails in a timely fashion.

5. Employees of the district are expected to check their e-mail on a frequent and consistent basis in order to stay current with district-related communications. It is recommended that e-mail be checked daily, but at a minimum, twice per week. Regular e-mail management will also minimize the risk that the inbox will be full, causing the e-mail to be returned to the sender with an error.

6. When an employee of the district is out of the office due to planned leave, such as vacation, they are to set their out-of-office assistant with a message explaining the duration of their absence and who to contact should immediate assistance be required.

7. Employees must ensure that there is sufficient space in their accounts to allow for e-mail to be delivered. Employees have the responsibility to recognize that certain communications may be time critical. Employees will not be held responsible for an interruption in their ability to access a message if system malfunctions or other system-related problems prevent timely delivery of, or access to, that message (e.g., power outages or e-mail system viruses).

8. Undeliverable messages returned because of a full inbox will be considered delivered without further action required of the district.

9. All building, districtwide and groups of employees, e-mail distribution lists will be established and maintained by the IT department.

10. Material sent to distribution lists must be related to the group being mailed and must pertain to district business. The distribution lists are not intended to be used for personal or commercial gain. All building or districtwide e-mails sent need prior approval.

11. Individuals may create convenience distribution lists as desired using their Outlook address book.

12. Districtwide and building e-mail distribution lists are not available to nondistrict entities.

Information Content/Third Party Supplied Information

1. System users and parents of student system users are advised that use of the district's system may provide access to materials that may be considered objectionable and inconsistent with the district's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the district's system accordingly.

2. Opinions, advice, services and all other information expressed by system users, information providers, service providers or other third party individuals are those of the providers and not the district.

3. System users may, with supervising teacher or system coordinator approval, order services or merchandise from other individuals and agencies that may be accessed through the district's system. These individuals and agencies are not affiliated with the district. All matters concerning merchandise and services ordered including, but not limited to, purchase terms, payment terms, warranties, guarantees and delivery are solely between the seller and the system user. The district makes no warranties or representation whatsoever with regard to any goods or services provided by the seller. District staff and administration shall not be a party to any such transaction or be liable for any costs or damages arising out of, either directly or indirectly, the actions or inactions of sellers.

4. The district does not warrant that the functions or services performed by or that the information or software contained on the system will meet the system user's requirements or that the system will be uninterrupted or error-free or that defects will be corrected. The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express or implied including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein.

Sheridan School District 48J

Responsible Technology Use Agreement

Students and Parents/Guardians: Please read this together, sign and return to the main office.

Statement of Purpose

Sheridan School District Staff and students use technology and internet-based tools (e.g., Google Apps for Education, Online Curriculum, online multimedia, etc.) in their classrooms on a regular basis to meet the district's standards and prepare students to live and work in the digital age. These technologies improve student communication and collaboration skills, provide a real audience, and extend learning beyond the classroom walls while building digital citizenship skills. Student access to technology will require responsible, courteous, efficient and legal use. Our goal in providing access to these resources is to enhance the education of our students and to educate them in responsible and appropriate use. It is important that students and parents recognize that information posted on the internet is public and permanent and needs to be appropriate.

Terms of Agreement

1. I agree to follow teacher/building/district instructions when using technology and will use technology carefully, productively, appropriately, and primarily for school-related purposes.
2. I agree to be polite, considerate, and to use appropriate language, I agree to never use technology to bully, abuse, harm or frighten others.
3. I agree to not search or view obscene or offensive materials, access inappropriate websites or engage in hacking or vandalism.
4. I agree to tell an adult if I read, see, or, access something inappropriate, or I witness inappropriate use of technology. I agree to not interfere with any filter or security measure.
5. I agree to use technology responsibly and to conserve school, district resources, such as server space, bandwidth, and printing capacity.
6. I agree to not share my passwords, except with my teacher or parent/guardian (FERPA). I agree that I will use complex passwords.
7. I agree to only use my own files and folders I will not access another individual's files and folders without their permission.
8. I agree that I will not reveal or post personal information belonging to myself or another person (i.e., passwords, address, telephone number, photos).
9. I agree to adhere to copyright laws and license and terms of use agreements.

Violations of Responsible Technology Use Agreement

- Suspension of computer privileges
- Notification of parent/guardian
- Detention, suspension, expulsions from school and school-related activities
- Legal action and/or prosecution

I understand that my use of any district technology (computer, network, internet, resources, etc.) will be monitored. I understand that if I violate this agreement, the district's policies and procedures, or student handbook, I may not be able to use technology or may experience other appropriate consequences. I acknowledge that my communications while using district technology (i.e. Google Apps) is neither private nor confidential.

Students and parent/guardian: By signing my name below I agree to these terms and I have read and discussed this Responsible Technology Use Agreement.

Student Signature _____ Date _____

Parent/Guardian Signature _____ Date _____

SHERIDAN SCHOOL DISTRICT 48J
AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT
(Nonschool System User)

I have read the district's Electronic Communications System policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions will result in suspension or revocation of system access and related privileges and/or referral to law enforcement officials.

In consideration for the privilege of using the district's Electronic Communications System and in consideration for having access to the public networks, I hereby release the district, its operators and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use or inability to use the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

_____ _____
Signature Date

_____
Home Address

_____
Home Phone Number

This space reserved for System Coordinator

Assigned Username: _____ Assigned Password: _____

Agreement for an Electronic Communications System Account
(Staff System User)

I have read the district's Electronic Communications System policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions will result in suspension or revocation of system access and related privileges, and may include discipline, up to and including dismissal and/or referral to law enforcement officials.

I understand that I may use my personal electronic device (PED) for education related purposes and that certain district proprietary information may be downloaded to my PED. I agree that any district proprietary information downloaded on my PED will only be as necessary to accomplish district purposes, obligations or duties, and will be properly removed from my PED when the use on my PED is no longer authorized. I insure that the personal electronic device in use is owned by me, and I am in complete control of the device at all times.

In consideration for the privilege of using the district's Electronic Communications System and in consideration for having access to the public networks, I hereby release the district, its operators and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use or inability to use the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

Signature _____

Home Address _____

Date _____ Home Phone Number _____

This space reserved for System Coordinator

Assigned Username: _____ Assigned Password: _____