Springfield School District 19

Code: **IIBGA-AR**
Revised/Reviewed: 8/10; 10/14; 2/09/15; 6/22/15; 8/08/16

Electronic Communications System - SpringNET

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. "SpringNet" as defined by the district is the system of communication devices (i.e. computers, telephones, and video systems) operated by the district for the purpose of transmitting and receiving various formats of digital and analog information.

7. "Vandalism" as defined by the district is any malicious attempt to harm or destroy district equipment, computer operating systems, applications software, or data.

General District Responsibilities

The district will:

1. Designate staff as necessary to ensure coordination and maintenance of SpringNET which includes all district computers, all network connected devices, all software, e-mail and Internet access;

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

3. Cooperate fully with local, state or federal officials in any investigation relating to misuse of SpringNET;

4. 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;

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

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

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

8. Provide staff supervision to monitor the online activities of students and staff 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;

9. 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;

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

11. Program its computers to display a message reinforcing key elements of the district's Electronic Communications System policy and regulation when accessed for use;

12. 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 is 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, the 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 from district servers. It is the responsibility of the individual staff member to insure that emails are retained in accordance with state archivist rules;

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 shared 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. Passwords should never be submitted, transmitted, or surrendered to any source inside or outside of the district. The one exception to this rule is an employee will provide passwords if requested by the superintendent or designee. Employees will take all reasonable precautions to protect passwords from others and will change passwords periodically;

13. Ensure all students, staff and nonschool system users complete and sign the SpringNet agreement stating that they will abide by the district's electronic communications policy and administrative regulations. Student and nonschool system users' agreements will be maintained on file in the school office. Staff agreements will be maintained on file at the district office.

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

System Access

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

   Board members, district employees, students in grades K-12 when under the direct supervision of staff, district volunteers, district contractors or other members of the public as authorized by the Superintendent or designee 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).

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, software, or file share music, videos or other materials 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 SpringNet 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, or to access restricted information, resources or networks to which the user has not been given access;
k. Giving your password(s) to others.

2. Guidelines/Etiquette

a. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and administrative regulations;
b. Protect password confidentiality. Passwords are not to be shared with others;
c. Report violations of the district's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator as appropriate.

3. Password Guidelines

a. To insure the security of data stored on SpringNet, system users need to maintain secure passwords to their accounts. Secure passwords should be at least 8 characters in length, contain a combination of capital and lower case letters, and contain at least one number.
b. Passwords should be changed periodically and at no time should the password be written down and stored in the proximity of the computer.

Complaints

Complaints regarding use of SpringNet may be made to the teacher, principal, employee's supervisor or system coordinator. The district's established complaint regulation will be used for complaints concerning violations of Board policy IIBGA and administrative regulation IIBGA-AR. See Board policy KL and accompanying administrative regulations.

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 regulations.

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 the Oregon Government Ethics Commission (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/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 or nondistrict, business related usage of the district's telephone system including district owned cellular telephones.

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.

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.

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.

Springfield Public Schools

Dear Parents:

Your student has the opportunity to use the district's electronic communications system which includes the Internet as part of their educational experience at Springfield Public Schools.

The Internet is a system that links communications networks creating a large and diverse network. Internet access gives your student the opportunity to reach out to many other people to share information, learn concepts, and research subjects by the sending and receiving of messages using the district computer network. The Internet will allow your student to communicate with other schools, colleges, organizations and individuals around the world.

With this educational opportunity also comes responsibility. It is important that you and your student read the enclosed Board Policy (IIBGA), Administrative Procedure (IIBGA-AR), and the agreement form, and that you discuss these requirements together. Violation of these rules will result in discipline including suspension or revocation of your student's access to the district's system, up to expulsion from school, as well as potential referral to law enforcement officials.

Although the district is committed to practices that ensure the safety and welfare of system users including the use of technology protection measures such as Internet filtering, please be aware that there still may be material or communications on the Internet that district staff, parents, and students may find objectionable. While the district neither encourages nor condones access to such material, it is not possible for us to eliminate that access completely.

Springfield Public Schools uses Google Applications for Education for student email, collaboration and communication. Google Applications for Education are provided to Springfield Public Schools under a Contract between the State of Oregon and Google. These sites allow us to set-up email accounts, calendars, and document creation tools for students. Your signature on this form provides the district, the state of Oregon and Google with acceptance of user guidelines that are reflected in the District Policies for educational use of electronic applications. The agreements in place for these services have been reviewed and approved by the Oregon Department of Education and our district. Our top priority is the safety of our students and their information. Teachers are provided with training on how to use these tools effectively. And our students will be receiving instruction in online safety, cyberbullying, and appropriate behavior on the Internet.

If you have any concerns about these tools or their use, or your student's access to the Internet, please feel free to contact your school principal.

Attached to this letter are the following important documents:

- The district's Electronic Communications System Policy (IIBGA) and Administrative Procedure (IIBGA-AR)
- An agreement for you and your student to read and sign stating that they have read IIBGA and IIBGA- AR and that they agree to follow IIBGA and IIBGA-AR. This agreement requires your signature. It must be signed each time your student enters a new Springfield school and will be kept on file at the school.

Please review these materials carefully with your student and return the attached agreement form to the school office.

Sincerely,

Superintendent

Springfield Public Schools

Student Agreement: Electronic Communications System Usage

1. Student Section

   Student Name _____ Grade _____

   School _____

   I have read the district's Electronic Communications System policy (IIBGA) and Administrative Procedure (IIBGA-AR), and I agree to abide by their provisions. I understand that violation of these rules will result in discipline up to and including expulsion from school, suspension and/or revocation of system access and related privileges, and potential referral to law enforcement officials.

   Student's Signature _____

   Date _____

2. Parent/Guardian

   I have read the district's Electronic Communications System policy (IIBGA) and Administrative Procedure (IIBGA-AR)

   _____ (Initials) I certify that the information contained on this form is correct. Further, 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, or my students use, or inability to use, the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

   Signature of Parent _____

   Home Address _____

   Date _____ Daytime Phone Number _____

This space reserved for District Use.

Date Received _____