Ashland School District 5

Code: **IIBGA-AR**
Revised/Reviewed: 12/01/04; 6/12/17
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.[1]

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.

[1]As inappropriate matter is not defined in the CIPA or regulations, districts should define the scope of what it will regard as inappropriate matter. The language provided in #5. is intended as a guide only.

General District Responsibilities

The district will:

1. Designate staff 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. A supervisor or other individual authorized by the superintendent may disable technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate, by completing the Form to Unblock Access to an Instructional Website;

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, social media, 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. 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.

14. 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 ;

15. 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, with parent approval and when under the direct supervision of staff and others with administrative approval.

2. Students, staff, Board members, volunteers, district contractors and other members of the public may be permitted to use the district's system for personal use, in addition to official district business, consistent with Board policy, general use prohibitions/guidelines/etiquette and other applicable provisions of this administrative regulation. Personal use of district-owned computers including Internet and E-mail access by employees is prohibited during the employee's work hours. Additionally, Board member and employee use of district-owned computers may be permitted only when such use does not violate the provisions of ORS 244.040 and use is under the same terms and conditions that access is provided to the general public under the district's policy governing use of district equipment and materials.

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 other 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 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 test 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, failure to provide the district with individual passwords or to access restricted information, resources or networks to which the user has not been given access.

2. Guidelines/Etiquette

Appropriate system use etiquette is expected of all users and is explained in district training sessions.

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 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 OAR 584-020-0041.
d. Violations of ORS 244.040 will be reported to 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.

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.

CO-80 4/22/03

Ashland Public Schools
Form to Unblock Access to an Instructional Web-Site

Name of teacher making request: _____

Date of Request: _____

Grade Level: _____ Subject Area: _____

Web-Site Address: _____

Rationale for allowing access to this site:

Explain why this information cannot be located at an alternate site:

Administrative Response:

☐ I do not authorize access to this site
☐ I authorize access to this site and am forwarding this form to the systems administrator to unblock access to this site.

_____ _____
Authorizing Administrator Signature Date

Ashland School District
User Agreement and Parent Permission Form

As a user of the Ashland School District's computer network, I hereby agree to comply with the above stated rules – communicating over the network in a responsible fashion while honoring all relevant laws and restrictions.

Student Signature _____ Date _____

As the parent or legal guardian of the minor student signing above, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet. I understand that individuals and families may be he held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use – setting and conveying standards for my son or daughter to follow when selecting, sharing or exploring information and media.

Parent Signature _____ Date _____

Name of Student _____ Birthdate _____

School _____ Grade _____ Soc Sec # _____

Street Address _____ Home Phone _____

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: _____

Home Address: _____

Date: _____ 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: _____