Linn Benton Lincoln
Education Service District

Code: **IIBGA-AR**

Revised/Reviewed: 5/9/2017

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 ESD schools.

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

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

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

General ESD Responsibilities

The ESD will:

1. Designate staff as necessary to ensure coordination and maintenance of the ESD's electronic communications system which includes all ESD computers, electronic devices, e-mail and Internet access;

2. Provide staff training in the appropriate use of the ESD's system including copies of ESD policy and administrative regulations;

3. Provide a system for authorizing staff use of personal electronic devices to download or access ESD proprietary information that insures the protections of said information;

4. Provide a system for obtaining prior written agreement from staff for the recovery of ESD proprietary information downloaded to staff personal electronic devices as necessary to accomplish ESD 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 ESD's system;

6. Use only properly licensed software, audio or video media purchased by the ESD or approved for use by the ESD. The ESD 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 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 to cyberbullying;

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

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

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

15. Notify appropriate system users that:

a. The ESD 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 ESD's information system are the ESD's property and are to be used for authorized purposes only. Use of ESD equipment or software for unauthorized purposes is strictly prohibited;
b. Files and other information, including e-mail, sent or received, generated or stored on ESD servers are not private and may be subject to monitoring. The ESD reserves the right to access and disclose, as appropriate, all information and data contained on ESD computers and ESDowned e-mail system;
c. The ESD currently retains all email, but 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 ESD's computers and e-mail system may become discoverable evidence if a public records request is made or a lawsuit is filed against the ESD. "Deleted" or "purged" data from ESD computers or e-mail system may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the ESD;
f. The ESD may set quotas for system disk usage;
g. Passwords used on the ESD's system are the property of the ESD and must be provided on Superintendent request.
h. Transmission of any materials regarding political campaigns is prohibited.

15. Ensure all staff complete and sign an agreement to abide by the ESD's electronic communications policy and administrative regulations. All such agreements will be maintained on file.

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

System Access

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

Board members, ESD employees, students enrolled in ESD school programs and when under the direct supervision of staff, ESD volunteers, ESD contractors or other members of the public as authorized by the system coordinator or ESD administrators consistent with the ESD's policy governing use of ESD equipment and materials.

2. Students, staff and Board members may be permitted to use the ESD's system to conduct business related to the management or instructional needs of the ESD or to conduct research related to education.
3. Staff members are allowed to use the ESD's internet system for personal electronic devices (personal cell phones, etc.) as outlined in Board policy GCAB.

General Use Prohibitions/Guidelines/Etiquette

Operation of the ESD'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 ESD's system.

1. Prohibitions

The following conduct is strictly prohibited:

a. Attempts to use the ESD'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 ESD's system in violation of copyright law or applicable provisions of use or license agreements;
c. Attempts to degrade, disrupt or vandalize the ESD's equipment, software, materials or data or those of any other user of the ESD's system or any of the agencies or other networks connected to the ESD'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 ESD;
(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 ESD'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 Program Administrator and consistent with applicable Board policy pertaining to student directory information, and personally identifiable information. Personal student 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 non-educational private student meetings is prohibited.
i. Attempts to use the ESD's name in external communication forums such as chat rooms without prior ESD authorization;
j. Attempts to use another individual's account name or password is prohibited.

2. Systems Users will

a. Protect network password confidentiality. Passwords are the responsibility of the employee 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;
b. Communicate only with such users and/or sites as may be authorized by the ESD;
c. Report violations of the ESD's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate;
d. Follow appropriate system etiquette as explained in ESD guidelines;
e. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and Administrative regulations.
f. Adhere to professional standards and scope of practice when arranging for private educationrelated meetings with students; and seek authorization from program administrators for unusual or incidental meetings.

Complaints

Complaints regarding use of the ESD's Electronic Communications System may be made to the Program Administrator or system coordinator. The ESD's established complaint procedure will be used for complaints concerning violations of the ESD'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 suspension of ESD 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.

2. Staff

    a. Staff who violate the General Use Prohibitions/Guidelines/Etiquette or the System Access sections of this document 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. Violation of applicable standards for non-TSPC licensing Boards will be repared
    e. Violations of ORS 244.040 will be reported to Oregon Government Ethics Commission (OGEC).

3. Others

    a. Other guest users who violate the General Use Prohibitions/Guidelines/Etiquette 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 ESD assumes no responsibility or liability for any membership, phone charges, or data access 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 ESD's system.

2. Any disputes or problems regarding phone services for home users of the ESD'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 ESD's system may provide access to materials that may be considered objectionable and inconsistent with the ESD's mission and goals. Parents should be aware of the existence of such materials and monitor their student's home usage of the ESD'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 ESD.

3. System users may, with program administrator or system coordinator approval, order services or merchandise from other individuals and agencies that may be accessed through the ESD's system. These individuals and agencies are not affiliated with the ESD. 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 ESD makes no warranties or representation whatsoever with regard to any goods or services provided by the seller. ESD 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 ESD 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 ESD's system is provided on an "as is, as available" basis. The ESD 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.