Linn Benton Lincoln
Education Service District

Code: **IIBGA-AR**
Reviewed: 7/21/2021

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 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 action 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 and sexual contact," as defined by CIPA, have the meanings given such terms in Section 2246 or 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 and the ESD's vision, mission and goals, as determined by the ESD.

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.

8. "Social Media" is defined as online, electronic or internet media, tolls, communities, and spaces

for social interaction, sharing user generated content, or public or semi-public communication.

General ESD Responsibilities

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 electronic communication 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 purposed, obligations or duties, and when the use of the personal electronic device is no longer authorized, to ensure 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 electronic communications system;

6. Social Media designated representative may only use sanctioned accounts on Twitter, Facebook, Instagram and YouTube.

7. Social Media designated representatives will be selected by each program director. They must meet the criteria listed in the Social Media Guidelines. They must complete the Social Media access form and be authorized by their director.

8. Use only properly licensed software, audio or video media purchase 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;

9. Install and use server virus detection and removal software;

10. 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;

11. Prohibit access by minors to inappropriate matter on the Internet and World Wide Web;

12. Provide staff supervision to monitor the online activities of students to prevent unauthorized access, including "hacking" and other unlawful activities online, and ensued the safety and security of

minors when authorized to use e-mail, social media, chat rooms, applications and other forms of direct electronic communication;

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

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

15. Determine which users will be provided access to the ESD's electronic communication system;

16. Program ESD computers to display a message reinforcing key elements of the ESD's electronics communication system policy and administrative regulation when accessed for use;

17. Notify appropriate system users that:

    a. The ESD retains ownership and control of its computers, hardware, software, and LBL social media sites and content 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. To maintain system integrity, monitor network etiquette and ensure that those authorized to use the ESD'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 ESD servers are not private and may be subject to monitoring. By using the ESD's system, individuals consent to have that use monitored by authorized ESD personnel. The ESD reserves the right to access and disclose, as appropriate, all information and date contained on ESD computers and ESD-owned e-mail system;
    c. The ESD currently retains all e-mail 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 be subject to disclosure 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 electronic communications system will be changed annually;
    h. Transmission of any communications or materials ~~regarding~~ related to activities prohibited by ORS 260.432 is not allowed.

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

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

Electronic Communications System Access

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

    a. Board members, ESD employees, and 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 Chief Information Technology Officer or ESD administrators consistent with the ESD's policy governing use of ESD equipment and materials.
    b. Staff and Board members may be permitted to use the ESD's electronic communications system to conduct business related to the management or instructional needs of the ESD or to conduct research related to education and when in compliance with Board policy and administrative regulations
    c. Personal use of the ESD's system or ESD-owned computers or devices including Internet and e-mail access by ESD staff [is prohibited may be permitted when consistent with Oregon ethics laws, Board policy and administrative regulations, when used on school property, and when on own time

General Use Prohibitions and Guidelines/Etiquette

Operation of the ESD's electronic communications 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 use of the ESD's system.

1. General Use Prohibitions

    The following conduct is strictly prohibited:
    a. Attempts to use the ESD's electronic communications 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 sue of 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 data usage quotas;
    e. Attempts to send, intentionally access or download any text file or picture or engage in any

communication that includes, but is not limited to, material which may be interpreted as:

1) Harmful to minors;
2) Obscene or child pornography as defined by law of indecent, vulgar, profane or lewd as determined by the ESD;
3) A product of service not permitted to minors by law;
4) Hazing, harassment, intimidation, bullying, menacing, threatening, act of cyberbullying; or a bias incident.
5) Constitutes insulting or fighting words, the very expression of which injures or harasses others, or which includes a symbol of hate;
6) A likelihood that, either because of its; content or the manner of distribution, it will cause a material or substantial disruption or the proper and orderly operation of the school of school activity;
7) 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 cost without specific approval. The user accessing such services will be responsible for these costs;
g. Attempts to post of publish personal student contact information unless authorized by the program director and consistent with applicable Board policy pertaining to student directory information, and personally identifiable information. Personal student contact information may include photograph, age, home, school, work or e-mail addresses of phone numbers of other unauthorized disclosure, use and dissemination of personal information regarding students;
h. Attempts to arrange student meetings with anyone on the ESD's electronic communications system, unless authorized by the program director CITO or when consistent with school or educational related activities when necessary;
i. Attempts to represent self on behalf of the ESD through use of the ESD's name in external communication forums, e.g., social media, chat rooms, without prior ESD authorization;
j. Attempts to use another individual's account name or password, failure to provide the ESD with individual passwords or to access restricted information, resources or networks to which the user has not been granted access.

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 CITO approval only;
   b. Report violations of the ESD's policy and administrative regulation or security problems to the supervising teacher, or ESD administrator, as appropriate;
   c. Follow appropriate system etiquette as explained in ESD guidelines;
   d. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and Administrative regulations.;
   e. Adhere to professional standards and scope of practice when using electronic mediums for

education related meetings; seek authorization from program director for unusual or incidental meetings;

f. When acting as a designated social media representative adhere to all LBL social media guidelines.

Complaints

The ESD's established complaint procedure in Board policy KL - Public Complaints and accompanying administrative regulation may be used to process complaints or concerns about violations of policy and 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 access up to the ESD electronic communications system access up to and including permanent loss of privileges.
    b. Violations of law may be reported to law enforcement officials and may result in criminal or civil sanctions.
    c. Disciplinary action may be appealed by parent, students and/or a representative in accordance with established ESD procedures.

2. Staff

    a. Staff who violate the General Use Prohibitions~~/~~ and 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. Violation of law may 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 may be reported to TSPC as provided by OAR 584-020-0041.
    d. Violation of applicable standards for non-TSPC licensing Boards may be reported.
    e. Violations of ORS 244-040 may be reported to Oregon Government Ethics Commission (OGEC).

3. Others
    a. Other guest users who violate the general electronic communications system user prohibitions shall be subject to suspension of system access up to and including permanent revocation of privileges.
    b. Violations of law may 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 or and/or equipment incurred by any home usage of the ESD's system.

2. Any disputes or problems resulting from phone services or internet provider services for home users of the ESD's electronic communications system are strictly between the system user and their internet service provider and/or phone 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 electronic communications system may provide access to materials that may be considered objectionable and inconsistent with the ESD's vision, mission and goals. Parents should be aware of the existence of such material and monitor their student's home usage of the ESD's electronic communications 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. Users of the electronic communications system may, with program director or CITO approval, order services or merchandise from vendors that may be accessed through the ESD's electronic communications system. These vendors 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 vendor and the electronic communications system user. The ESD makes no warranties or representation whatsoever with regard to any goods or service provided by the vendor. 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 vendor.

4. The ESD does not warrant that the functions or services performed by, or that the information or software contained on, the electronic communications system will meet the system user's requirements, or that the electronic communications system will be uninterrupted or error-free, or that defects will be corrected. The ESD's electronic communications 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 electronic communications system and any information or software contained therein.

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

I have received notice of, read and agree to abide by the provisions in the ESD's electronic communications system policy and administrative regulation and agree to abide by their provisions. I understand that violation of these provisions may result in suspension and/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 ESD proprietary information may be downloaded to, my PED. I agree that any ESD proprietary information downloaded on my PED will only be as necessary to accomplish ESD purposes, obligations or duties, and will be properly removed from my PED when the use on my PED is no longer authorized. I ensure that the PED 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 ESD's electronic communications system and in consideration for having access to the public networks, I hereby release the ESD, 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 ESD's policy and administrative regulation.

Signature_____ Date _____

Email Address_____

Home Phone Number_____ Cell Number_____

This space reserved for System Coordinator

Assigned Username:_____ Assigned Password:_____