

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, that is inconsistent with general public education purposes, the district’s mission and/or goals.

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

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. 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 principal may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate;
6. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet;
7. 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;
8. Provide student education about appropriate online behavior, including cyberbullying awareness and response, and how to interact with other individuals on social networking sites and in chat rooms;
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. 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, 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’s 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 data storage. 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.
- h. Transmission of any materials regarding political campaigns is prohibited.

12. 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 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.

OR

2. 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. Personal use of district-purchased electronic devices (i.e. computers, tablets, mobiles) must also comply with IRS regulations. Personal use of such devices that are not regularly used in the district for instructional or business purposes must be reported annually to the district on a form prescribed by the Director of Finance.

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) Unauthorized sale or purchase of merchandise and services;
- (3) Collection of signatures;
- (4) Membership drives;
- (5) Transmission of any materials regarding political campaigns;
- (6) Any other activity expressly prohibited by Board policy, state or federal statute.

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 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 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;
- g. Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization;
- h. 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

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 the privacy of others.
 - (1) Do not read the mail or files of others without their permission;
 - (2) Users will not repost a message that was sent to them privately without permission of the person who sent them the message.
 - (3) Users will not post private information about another person.
- c. Remember, there is no expected right to privacy when using e-mail;
- d. 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;

- e. Report violations of the district's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate.

Personal safety restrictions for students:

1. Students will not post personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, etc.
2. Students will not agree to meet with someone they have met online without their parent's approval and participation.
3. Students will promptly disclose to their teacher or other school employee any message or image they receive that they deem inappropriate or makes them feel uncomfortable.

Websites

1. District website restrictions:
 - a. The district will establish a website on which all authorized information regarding district programs and services will be posted. Material appropriate for placement on the district website includes: district information, school information, teacher or class information, student projects, and student extracurricular organization information. Personal, noneducationally related information will not be allowed on the district website.
 - b. The district superintendent will designate a district web publisher, responsible for maintaining the official district website and monitoring all district web activity. The web publisher will develop style and content guidelines for official district and school web materials and develop procedure for the placement and removal of such material. All official district material originating from the district posted on the district website must be approved through a process established by the district web publisher.
2. School web pages: The principal will designate a school web publisher, responsible for managing the school website and monitoring class, teacher, student and extracurricular web pages. All official material originating from the school will be consistent with the district style and content guidelines and approved through a process established by the school web publisher. The school web publisher will develop additional guidelines for the school website, as needed.
3. Teacher web pages: Teachers may establish web pages for use with class instructional activities or that provide a resource for other teachers. Teachers will be responsible for maintaining their class or education resource sites. Teacher web pages will not be considered official material, but will be developed in such a manner as to reflect well upon the district and school.
4. Staff web pages: Staff may develop web pages that provide a resource for others. Staff will be responsible for maintaining their resource sites. Staff web pages will not be considered official material, but will be developed in a manner as to reflect well upon the district.
5. Student web pages:
 - a. Students may create a website as part of a class activity. Material presented on a student class activity website must meet the educational objectives of the class activity.

- b. With the approval of the principal or web publisher, students may establish personal web pages. Material presented in the student's personal website must be related to the student's educational and career preparation activities.
- c. It will not be considered a violation of the student's right to free speech to require removal of material that fails to meet established educational objectives or that is in violation of a provision of the district technology use regulations or student disciplinary code. However, student material may not be removed on the basis of disagreement with the views expressed by the student.

6. Extracurricular organization web pages:

- a. With the approval of the principal, extracurricular organizations may establish web pages on the district website. Material presented on the organization web page must relate specifically to organization activities.
- b. Organization web pages must include the following notice:

This is a student extracurricular organization web page. Opinions expressed on this page shall not be attributed to the ESD or district.

7. Web page information:

- a. All district technology use regulations apply to material placed on the web.
- b. "Directory Information," is defined as items of personally identifiable information contained in the educational records of students which would not be generally considered harmful or an invasion of privacy if disclosed. The following directory information may be placed on web pages: student's first and last name, photograph(s), participation in officially recognized activities and sports; weight and height if a member of an athletic team(s); grade level; dates of attendance; degrees and awards received; and school of record.

The district shall provide written annual notice to parents of students currently in attendance, and eligible students in attendance, of their right to provide the district with a written directive to not disclose directory information. The district shall effectively notify and receive directives from parents of students, and eligible students whose primary or home language is other than English.

- c. Web pages shall not:
 - (1) Contain the address, phone number(s) and date and place of birth of students currently in attendance;
 - (2) Contain copyrighted or trademarked material belonging to others unless written permission to display such material has been obtained from the owner. There will be no assumption that the publication of copyrighted material on a website is within the fair use exemption.
- d. Material placed on the website is expected to meet academic standards for proper spelling, grammar and accuracy of information.
- e. Students may retain the copyright on the material they create that is posted on the web. Web material developed by employees during regular work hours is the property of the district and may be copyrighted by the district. Material developed by employees, while not under contract, may be copyrighted by the employee, but posted to the web only with the permission of the district web publisher.

8. Users should retain a back-up copy of their web pages.

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 GSPC.
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.