

## Electronic Communications System

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 district policy and this administrative regulation, minor will include all students enrolled in district schools.
5. “Inappropriate Material” is any material that violates CIPA regulations, and textual or audio descriptions which are obscene, child pornography, or harmful to minors. Inappropriate material is also any material that has no or little real educational value or is inconsistent with the district’s mission and goals.

### District Responsibilities

The district will:

1. 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;
2. Cooperate fully with local, state, or federal officials in any investigation relating to misuse of the district’s system;

3. 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;
4. Install and use desktop and/or server virus detection and removal software;
5. Provide technology protection measures that protect against Internet access by both adults and minors to inappropriate material. The electronic communications director or coordinator 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 to inappropriate material;
7. 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;
8. Provide staff supervision to monitor online activities to prevent unauthorized access or "hacking" online and ensure the safety and security of minors authorized to use email, chat rooms and other forms of electronic communications.
9. Ensure that all 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 electronic communications office.
10. Notify users of known copyright infringing activities and deny access to or remove the material.

### **System Access**

Access to the district's system is granted to Board members, district employees, students in grades K-12, with parent or legal guardian approval and when under the direct supervision of staff, or other members of the public as authorized by the electronic communications director or coordinator.

### **User Notifications**

1. 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 electronic communications director or coordinator or their authorized designee(s) may routinely review, monitor, copy, and/or log user files and communications.
2. 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 the electronic communications director or coordinator or their

authorized designee(s). The district reserves the right to access and disclose, as appropriate, all information and data contained on district computers.

3. Information and data entered or stored on the district's computer systems 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 computer systems may be retrieved for later public records disclosure or disciplinary purposes, as deemed necessary by the district.
4. Any computer system brought onto district property will be subject to the same rules and regulations as a district-owned computer system.
5. System users and parents of student system users are advised that the 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 that complete filtering or removal of such material is impossible, but that every effort is made to limit access to such material as much as possible. If a parent has a specific complaint they are encouraged to bring the offending material to the attention of the electronic communications director or coordinator.
6. 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.
7. System users may, with supervising teacher or electronic communications director or 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.
8. 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 expressed 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.

### **General Acceptable System Use**

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. 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 or services;
  - (4) Collection of signatures;
  - (5) Membership drives;
  - (6) Transmission of any materials regarding political campaigns.
- b. Attempts to upload, download, use, install, reproduce, store or distribute information, data, or 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 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 electronic communications director or coordinator 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 electronic communications director or 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, fail 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. The system users will:
    - a. Adhere to the same standards for communicating on-line that are expected in the classroom and consistent with the Board policy and administrative regulations;
    - b. Respect other people's time and cyber space. Use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher, administrator or electronic communications director or coordinator. Avoid downloading excessively large files. Remain on the system long enough to get needed information then exit the system. Act as though every byte sent costs somebody time and money, because it does;
    - c. Respect the privacy of others. Do not read the mail or files of others without their permission;
    - d. Cite all quotes, references, and sources;
    - e. 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, administrator, or electronic communications Director or coordinator approval only. No user may use a password on the district's systems that are unknown to the district;
    - f. Communicate only with such users and/or sites as may be authorized by the district;
    - g. Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques;
    - h. Report violations of the law, district's policy, administrative regulation, or security problems to the supervising teacher, administrator, or electronic communications director or coordinator as appropriate.

### **Student Acceptable System Use**

In addition to the prohibitions and guidelines defined in the General Acceptable System Use section, students must also abide by the following regulations:

1. Student access the system is a privilege, and may be restricted or revoked at any time;
2. Students are strictly prohibited from:
  - a. Using district computers or services for any purpose other than the completion of class work, school-related research, or other research which will further their educational and/or professional goals;
  - b. Using district computers to access E-mail, chat, Instant Messaging, or any other communication service except with specific teacher, administrator, or electronic communications Director or coordinator permission and only for the completion of class work, school-related research, or other research which will further their educational and/or professional goals;
  - c. Using encryption or tunneling technologies for any reason. It must be stressed that violation of this regulation constitutes a serious offense and carries significant disciplinary consequences.

## Staff and Board Member Acceptable System Use

In addition to the prohibitions and guidelines defined in the General Acceptable System Use section, staff and Board members must also abide by the following regulations:

1. Staff 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 and expectations 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 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 OAR 584-020-0041 and use is under the same terms and conditions that access is granted to the general public under the district's policy governing use of district equipment and materials.
2. Staff is encouraged to use encryption or tunneling technologies as appropriate to protect sensitive information from unauthorized access. However, use of such technologies to obscure prohibited activities or to keep information or communication from being monitored by authorized personnel is strictly prohibited. Disclosure of passwords or encryption keys to the electronic communications Director or coordinator upon request is required. It must be stressed that violation of this regulation constitutes a serious offense and carries significant disciplinary consequences.

## Complaints

Complaints regarding use of the district's electronic communications system may be made to the teacher, administrator, employee's supervisor or electronic communications director or coordinator. The district's established complaint procedure will be used for complaints concerning violations of the district's electronic communications policy and/or 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.

Name: \_\_\_\_\_ Position: \_\_\_\_\_

School: Elmira Elem Veneta Elem FRMS EHS Department: \_\_\_\_\_

By signing this form I acknowledge that I have read the attached synopsis and a copy of the district's Internet Policy IIBGA and accompanying rules and regulations are available to me.

I understand that violation of the district's Acceptable Use of the Internet & Internet Safety Policy will be handled in accordance with district policy, rules and regulations and any other governing instruments such as the current collective bargaining agreement.

\_\_\_\_\_  
FRSD Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor's Signature

\_\_\_\_\_  
Date

\*\*\*\*\*

This space for Technology Coordinator's notes:

The district has developed policies and procedures for use of the Internet by students, staff and guests. Following is a synopsis of the rules that apply to all Internet users.

1. Internet use is to be limited to classroom curriculum activities, professional or career development and limited high-quality personal research.
2. Internet is not to be used for commercial purposes. Commercial Purposes indicates that one should not purchase or offer for purchase or provide products through the Internet. Exceptions for specific classroom or extra-curricular activities must first be obtained from the superintendent or the superintendent's designee.
3. Users are not to use or access obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or graphics. A person(s) who has used or accessed obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or graphics will be subject to discipline including but not limited to expulsion or position termination.
4. Users are not to harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
5. Users are not to engage in personal attacks or knowingly or recklessly post false or defamatory information about another person or organization.
6. Users have a limited privacy expectation of the content in computer files and records of online activity. The district reserves the right to inspect any computer system or file.
7. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or district policy.
8. Users are not to attempt to gain unauthorized access to the district system or any other system through the use of the district network or go beyond their authorized access. This includes attempting to log in through another person's account or access to another person's files.
9. Users are not to make deliberate attempts to disrupt a computer system's performance or destroy data by spreading any computer virus or by any other means. Such actions are illegal and will be prosecuted to the full extent of the law.
10. Users will notify the system administrator or supervising teacher when they see a possible security problem.
11. Users are to obey all copyright laws with regard to downloading of files or reproduction of any materials found on the Internet.
12. Users will not download and/or install software without prior approval from the District Technology Coordinator.

**Web Pages:**

1. Users will not post the full name or identifiable picture of any student without written parent permission.
2. All web pages are to be pre-approved by the appointed District Webmaster prior to the web page being published.

Fern Ridge School District  
District Office  
88834 Territorial Road  
Elmira, OR 97437

**Internet Account Agreement  
Web Picture Publishing  
Student Permission Form**

Student Name \_\_\_\_\_ Grade 6 7 8 9 10 11 12  
School \_\_\_\_\_ Academic Year \_\_\_\_\_

I agree to follow the district's rules. I understand that if I violate the rules my account can be terminated and I may face other disciplinary measures at school and legally. I understand that if I am provided an Electronic Mail account, it may be discontinued over the summer recess unless other arrangements are made with the System Coordinator.

Student Signature \_\_\_\_\_ Date \_\_\_\_\_

**Parent or Guardian:**

I have read the synopsis of the rules and regulations of the district's Internet Policy IIBGA "Appropriate Use of the Internet," as found on the back of this form. I hereby release the district, its personnel, and any institutions with which the district is affiliated, from any and all claims and damages of any nature arising from my child's use, or inability to use, the district system, including, but not limited to, claims that may arise from the unauthorized use of the system to purchase products or services. I further understand that I can be held liable for damages caused by my child, whether intentional or unintentional misuse of the district's computer(s) or computer system.

I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set forth in the district Acceptable Use Policy. I will emphasize to my child the importance of following rules for personal safety.

I understand that by checking the box marked Internet Use, and signing above the line next to the box, I am giving permission for my child to use the Internet and be given an electronic mail account if appropriate for school activities.

I understand that by checking the box marked Photo on School Web Page, and signing on the line next to this box, I am giving permission for my child's picture and first name to be posted on the school's web page if appropriate for school activities.

Please check the appropriate box(s) below to grant permission and sign on the concurrent line.

Internet Use                      Parent Signature                      Date \_\_\_\_\_  
 Photo on Web Page              Parent Signature                      Date \_\_\_\_\_

\_\_\_\_\_  
Parent's name (please print)                      Daytime Phone: \_\_\_\_\_  
\*\*\*\*\*

This space for Technology Coordinator's notes:

Building Staff Authorization: Date \_\_\_\_\_

The district has developed policies and procedures for use of the Internet by students, staff and guests. Following is a synopsis of the rules that apply to all Internet users.

1. Internet use is to be limited to classroom curriculum activities, professional or career development and limited high-quality personal research.
2. Internet is not to be used for commercial purposes. Commercial Purposes indicates that one should not purchase or offer for purchase or provide products through the Internet. Exceptions for specific classroom or extra-curricular activities must first be obtained from the superintendent or the superintendent's designee.
3. Users are not to use or access obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or graphics. A person(s) who has used or accessed obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or graphics will be subject to discipline including but not limited to expulsion or position termination.
4. Users are not to harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
5. Users are not to engage in personal attacks or knowingly or recklessly post false or defamatory information about another person or organization.
6. Users have a limited privacy expectation of the content in computer files and records of online activity. The district reserves the right to inspect any computer system or file.
7. An individual search will be conducted if there is reasonable suspicion that a user has violated the law or district policy.
8. Users are not to attempt to gain unauthorized access to the district system or any other system through the use of the district network or go beyond their authorized access. This includes attempting to log in through another person's account or access to another person's files.
9. Users are not to make deliberate attempts to disrupt a computer system's performance or destroy data by spreading any computer virus or by any other means. Such actions are illegal and will be prosecuted to the full extent of the law.
10. Users will notify the system administrator or supervising teacher when they see a possible security problem.
11. Users are to obey all copyright laws with regard to downloading of files or reproduction of any materials found on the Internet.
12. Users will not download and/or install software without prior approval from the District Technology Coordinator.

**Web Pages:**

1. Users will not post the full name or identifiable picture of any student without written parent permission.

- 
2. All web pages are to be pre-approved by the appointed District Webmaster prior to the web page being published.