

## Electronic Communications System

### 1. Definitions

- a. “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:
  - (1) Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
  - (2) Child pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
  - (3) Harmful to minors.
- b. “Harmful to minors” as defined by CIPA means any picture, image, graphic image file or other visual depiction that:
  - (1) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;
  - (2) 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
  - (3) Taken as a whole, lacks serious literary, artistic, political or scientific value to minors.
- c. “Sexual act; sexual contact” as defined by CIPA have the meanings given such terms in Section 2246 of Title 18, United States Code.
- d. “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.
- e. “Inappropriate matter” as defined by the district means material that is inconsistent with general public education purposes, the district’s mission and goals.

### 2. General District Responsibilities

The district will:

- a. 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.
- b. 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.

- c. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the district's system.
- d. 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.
- e. Install and use desktop and/or server virus detection and removal software.
- f. 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. An administrator, 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.
- g. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web.
- h. Provide staff supervision to monitor the on-line activities of students to prevent unauthorized access, including "hacking" and other unlawful activities on-line, and ensure the safety and security of minors when authorized to use E-mail, chat rooms and other forms of direct electronic communication.
- i. 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.
- j. Determine which users will be provided access to the district's E-mail system.
- k. Program its computers to display a message reinforcing key elements of the District's Electronic Communications System policy and regulation when accessed for use.
- l. Notify appropriate system users that:
  - (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, school administrators may routinely review 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 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.
  - (3) The district may establish a retention schedule for the removal of E-mail.
  - (4) 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.
  - (5) 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.

- (6) The district may set quotas for system storage 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.
  - (7) 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.
  - (8) Transmission of any materials regarding political campaigns is prohibited.
- m 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.

### 3. Technical Services Which May Be Provided Through District System

- a. E-mail will allow employees and students to communicate with people from throughout the world. Users will also be able to subscribe to mail lists to engage in group discussions related to educational subjects.
- b. World Wide Web provides access to a wide range of information in the form of text, graphics, photographs, video, and sound from throughout the world. The Web is a valuable research tool for students and employees.
- c. News groups are discussion groups that are similar to mail lists. The district will provide access to selected news groups that relate to subjects that are appropriate to the educational purpose of the system.

### 4. Access to the System

- a. Access to the district's system is authorized to Board members, district employees, students in grades K-8, 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. Students in grades 9-12 . . . (See student handbook).
- b. 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 should be limited to non-contract or non-duty hours and must not interfere with teaching or other district job responsibilities. Personal use is limited to occasional use (i.e., to write a letter or E-mail to a friend or family member) and is not to be used to avoid personal expense for a home or private Internet account. 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.
- c. Every person who has an individual account for using the Silver Falls Schools' network must have read the acceptable use agreement.

- d. Individual E-Mail Accounts for Students. At some point, students may be provided with individual E-mail accounts. The district will not provide students with dial-up access to the district network. An agreement will be required for an individual E-mail account. The student must sign this agreement and his or her parent before the account is approved.
- e. Individual E-Mail Accounts for District Employees. District employees will be provided with an individual account and may have dial-up access to the network at some point. All employees must sign an agreement acknowledging understanding of the district's acceptable use policy in order to obtain an account.
- f. Classroom E-Mail Accounts. In some instances, students will be granted E-mail access only through a classroom account used by all students in a given classroom and closely supervised by the teacher. No signed agreement will be required for a classroom account. An agreement will only be required for an individual account. Parents may specifically request that their child(ren) not be provided access through the classroom account by notifying the district in writing.
- g. Guest Accounts. Guests may receive an individual account with the approval of the district technology director if there is a specific, district-related purpose requiring such access. Use of the system by a guest must be specifically limited to the district-related purpose. An agreement will be required and parental signature will be required if the guest is a minor.

## 5. 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.

### a. Prohibitions

The following conduct is strictly prohibited:

- (1) Attempts to use the district's system for:
  - (a) Unauthorized solicitation of funds.
  - (b) Distribution of chain letters.
  - (c) Unauthorized sale or purchase of merchandise and services.
  - (d) Collection of signatures.
  - (e) Membership drives.
  - (f) Transmission of any materials regarding political or religious persuasion.
- (2) 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.
- (3) 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.
- (4) Attempts to evade, change or exceed resource quotas or disk usage quotas.

- (5) 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:
  - (a) Harmful to minors.
  - (b) Obscene or child pornography as defined by law or indecent, vulgar, profane or lewd as determined by the district.
  - (c) A product or service not permitted to minors by law.
  - (d) Harassment, intimidation, menacing, threatening or constitutes insulting or fighting words, the very expression of which injures or harasses others.
  - (e) 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.
  - (f) 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.
- (6) 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.
- (7) 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.
- (8) 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.
- (9) Attempts to use the district's name in external communication forums such as chat rooms without prior district authorization.
- (10) 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.

b. Guidelines/Etiquette

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

- (1) Adhere to the same standards for communicating on-line that are expected in the classroom and consistent with Board policy and administrative regulations.
- (2) Respect other people's time and cyberspace. Use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher or system coordinator. Avoid downloading excessively large files. Remain on the system long enough to get needed information then exit the system.
- (3) Take pride in communications. Check spelling and grammar.

- (4) Respect the privacy of others. Do not read the mail or files of others without their permission.
- (5) Cite all quotes, references and sources.
- (6) Adhere to guidelines for managing and composing effective E-mail messages:
  - (a) One subject per message - avoid covering various issues in a single E-mail message.
  - (b) Use a descriptive heading.
  - (c) Be concise - keep message short and to the point.
  - (d) Write short sentences.
  - (e) Use bulleted lists to break up complicated text.
  - (f) Conclude message with actions required and target dates.
  - (g) Remove E-mail in accordance with established guidelines.
  - (h) Remember, there is no expected right to privacy when using E-mail. Others may read or access mail.
  - (i) Always sign messages.
  - (j) Always acknowledge receipt of a document or file.
- (7) 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.
- (8) Communicate only with such users and/or sites as may be authorized by the district.
- (9) Be forgiving of the mistakes of others and share your knowledge. Practice good mentoring techniques.
- (10) Report violations of the district's policy and administrative regulation or security problems to the supervising teacher, system coordinator or administrator, as appropriate.

c. 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 regulations.

d. 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.

e. Telephone/Membership/Other Charges

f. The district assumes no responsibility or liability for any membership or phone 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 district's system.

g. Any disputes or problems regarding phone services for home users of the district's system are strictly between the system user and his/her local phone company and/or long distance service provider.

6. Information Content/Third Party Supplied Information

- a. 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.
- b. 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.
- c. 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.

- d. 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.

## 7. Web Sites

- a. Rights to Privacy. The district and its users will not include any reference to district personnel or users, including their names and pictures, without the individual's permission.
- b. Web Page Authorship. If a person or class Web page is created, a notice must be included to inform the public that the opinions expressed on the page are those of the creator of the Web page, not the district. A statement on the Web page must acknowledge the authorship of the page.
- c. District Web Site. The district will establish a Web site and will develop Web pages that will present information about the district. The district webmaster will be responsible for maintaining the district web site.
- d. School or Class Web Pages. Schools and classes may establish Web pages that present information about the school or class activities. The building principal and webmaster will designate an individual to be responsible for managing the school Web site. Teachers will be responsible for maintaining their class site.
- e. Student Web Pages. Students may be allowed to establish personal Web pages. This will only be done with the approval of the building principal. The district will form a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented in the student's Web site must be related to the student's educational and career preparation activities.
- f. Staff Web Pages. With building principal or designee approval, staff members will be allowed to establish Web pages for educational purposes. Any Web page that a staff member creates in his/her employment or individual capacity that is open to the general public is a reflection of that staff member and is to present an acceptable image and at all times serve as a role model to students.
- g. Extracurricular Organization Web Pages. With the approval of the school principal, extracurricular organizations may establish Web pages. The principal will form a process and criteria for the establishment and posting of material, including pointers to other sites, on these pages. Material presented on the organization Web page must relate specifically to organization activities and will include only student-produced material.
- h. Access. Users will not use "Web Chat Rooms," "Social Network Sites" or other new Web related technology without prior approval of the school principal or designee. Users with personal computing devices will be granted only wireless and guest access to the district network.

## 8. District Acceptable Use Policy

### a. Student Personal Safety

- (1) Students will not post personal contact information about themselves. Personal contact information includes address, telephone, home address, work address, etc. School address and E-mail address may be used when it is necessary to receive information.
- (2) Students will not post personal contact information about other people, including address, telephone, home address, work address, etc. In addition, the district and its users will not include any reference to district personnel or users, including their names and pictures, without their permission.
- (3) Students will not agree to meet with someone they have met on line without a parent's approval and participation.
- (4) Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

### b. Illegal or Destructive Activities

- (1) Users will not attempt to gain unauthorized access to the district network or any other computer system through the district network or to go beyond their authorized access. This includes attempting to log in through another person's account or to access another person's files.
- (2) Users will not make deliberate attempts to disrupt any computer system performance or to destroy data.
- (3) Users will not use the district network to engage in any other illegal act.

### c. System Security

- (1) Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.
- (2) Users will immediately notify the district network administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- (3) Users will avoid the inadvertent spread of computer viruses by following the district virus protection procedures if they download software.

### d. Inappropriate Conduct

- (1) Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
- (2) Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- (3) Users will not post information that, if acted upon, could cause damage or danger of disruption.
- (4) Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

- (5) Users will not harass another person. Harassment is acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, the user must stop.
  - (6) Users will not post false or defamatory information about a person or organization.
- e. Respect for Privacy
- (1) Users will not repost a message that was sent to them privately.
  - (2) Users will not post personal contact information about other people, including address, telephone, home address, work address, etc. In addition, the district and its users will not include any reference to district personnel or users, including their names and pictures without their permission.
- f. Respecting Resource Limits
- (1) Users will use the network only for educational and professional or career development activities and limited, high-quality, self-discovery activities.
  - (2) Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the network is not being heavily used and immediately remove the file from the network system computer to their personal computer.
  - (3) Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.
  - (4) Users will check their E-mail frequently, delete unwanted messages promptly, and stay within their E-mail quota.
  - (5) Users will subscribe only to high-quality, discussion-group mail lists that are relevant to their education or professional/career development.
  - (6) Users will unsubscribe to discussion groups before any vacation, break, or other extended absence from school.
- g. Plagiarism and Copyright Infringement
- (1) Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
  - (2) Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not he/she can use a work, he/she should request permission from the copyright owner.
- h. Inappropriate Access to Material
- (1) Users will not use the district network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). Exceptions may be made if the purpose of such access is to conduct research and if both the teacher and the parent approve access.
  - (2) If a user inadvertently accesses such information, he/she should immediately disclose the inadvertent access in a manner specified by their school.

9. Due Process

- a. In the event there is an allegation that a student has violated the district acceptable use policy, the student will be provided with notice of the alleged violation and an opportunity to present an explanation before an administrator.
- b. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of regulations in the Student Handbook, the violation will be handled in accord with the applicable regulation of the Student Handbook.
- c. Any district administrator may terminate the account privileges of a guest user by providing notice to the user. Guest accounts not active for more than 30 days may be removed, along with the user's files, without notice to the user.

---

## ACCEPTABLE USE POLICY AND AGREEMENT

---

### EDUCATIONAL PURPOSE:

The Silver Falls School District's network and the Internet offer a wealth of educational materials to our students and teachers. Original source materials, information, data, images, and computer software may be brought into the classroom. Access to the Internet is an important part of our plan to create lifelong learners who know how to find information in our rapidly changing world. Internet access makes contact with people all over the world possible, bringing into the classroom experts in every content area. Teachers can use these resources for individual and group projects, curricular materials, and idea sharing. Expertise in our schools may be shared with others around the world. Educators may share lesson plans and may network to enrich their skills.

### ACCEPTABLE USE POLICY:

1. Students' Personal Safety
  - a. Students will not post personal contact information about themselves. Personal contact information includes address, telephone, home address, work address, etc. School address and E-mail address may be used when it is necessary to receive information.
  - b. Students will not post personal contact information about other people, including address, telephone, home address, work address, etc. In addition, the district and its users will not include any reference to district personnel or users, including their names and pictures, without their permission.
  - c. Students will not agree to meet with someone they have met on line without their parents' approval and participation.
  - d. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
2. Illegal or Destructive Activities
  - a. Users will not attempt to gain unauthorized access to the district network, or to any other computer system through the district network, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
  - b. Users will not make deliberate attempts to disrupt any computer system performance or destroy data.
  - c. Users will not use the district network to engage in any other illegal act.
3. System Security
  - a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.
  - b. Users will immediately notify the district network administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
  - c. Users will avoid the inadvertent spread of computer viruses by following the district virus protection procedures if they download software.

#### 4. Inappropriate Conduct

- a. Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
- b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.
- d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- e. Users will not harass another person. Harassment is acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, the user must stop.
- f. Users will not post false or defamatory information about a person or organization.
- g. Users will not engage in cyberbullying or any form of communication which disrupts or prevents a safe and positive educational or working environment.

#### 5. Respect for Privacy

- a. Users will not re-post a message that was sent to them privately.
- b. Users will not post personal contact information about other people, including address, telephone, home address, work address, etc. In addition, the district and its users will not include any reference to district personnel or users, including their names and pictures, without their permission.

#### 6. Respecting Resource Limits

- a. Users will use the network only for educational and professional or career development activities, and limited, high-quality, self-discovery activities.
- b. Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the network is not being heavily used and immediately remove the file from the network system computer to their personal computer.
- c. Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.
- d. Users will check their E-mail frequently, delete unwanted messages promptly, and stay within their E-mail quota.
- e. Users will subscribe only to high-quality discussion group mail lists that are relevant to their education or professional/career development.
- f. Users will unsubscribe to discussion groups before any vacation, break, or other extended absence from school.

#### 7. Plagiarism and Copyright Infringement

- a. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

8. Inappropriate Access to Material

- a. Users will not use the district network to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). Exceptions may be made if the purpose of such access is to conduct research, and if both the teacher and the parent approve access.
- b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school.

9. Web Sites

- a. The district and its users will not include any reference to district personnel or users, including their names and pictures, without the individual's permission.
- b. If a person or class Web page is created, a notice must be included to inform the public that the opinions expressed on the page are those of the creator of the Web page, not the district. A statement on the Web page must acknowledge the authorship of the page.
- c. Users will not use "Web Chat Rooms" or other new Web related technology without prior approval from the school principal or designee.

10. Due Process

- a. In the event there is an allegation that a student has violated the district acceptable use policy and agreement, the student will be provided with notice of the alleged violation and an opportunity to present an explanation before an administrator.
- b. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of regulations in the Student Handbook, the violation will be handled in accordance with the applicable regulation of the school or Student Handbook.