Grants Pass School District 7

Code: **IIBGA-AR**
Adopted: 5/14/02
Readopted: 2/24/04; 6/12/07; 3/11/08; 6/10/08; 5/25/10; 8/13/13; 9/08/15
Orig. Code(s): IIBGA-AR

Electronic Communications System Acceptable Use Regulation

The purpose of the Grants Pass School District No. 7 Network Acceptable Use Regulation is to ensure that all use of the District network is consistent with the mission and goals of the district's technology plan and meets the requirements of the Children's Internet Protection Act (CIPA). The term the District network refers to the District's electronic communication system which includes computers, email, Internet access, applications, and any physical or wireless technology access to the network both on and off district property.

The Board supports use of Local, Intranet and Internet networks in the District's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

All internet access on District operated resources will be filtered through the use of filtering software to prevent access by minors/parents/staff/outside users to inappropriate matter on the Internet and World Wide Web.

General District Responsibilities

The District will:

1. Provide technology protection measures that protect against Internet access by both adults and minors to visual depictions, text, or sound clips that are obscene, pornographic, or are determined to be harmful to minors. The superintendent or his designee may disable the technology protection measures to enable access for bona fide research or other lawful purposes, as deemed appropriate.

2. Prohibit access by minors, as defined by CIPA and this regulation, to inappropriate matter on the Internet and World Wide Web.

3. 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.

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

5. Protect users of the network from harassment or unwanted or unsolicited communications, to the greatest extent possible.

6. Determine which sites accessible as part of the District network are most applicable to the curricular needs of the District and may restrict user access, accordingly.

7. 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 network are in compliance with Board policy, administrative regulations and law, the Superintendent or the Superintendent's designee 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 network, 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, including any information or data contained within e-mail stored on District servers.
   c. Information and data entered, stored or received 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. E-mail sent or received within the District network is considered a public record and subject to state archivist rules for retention and destruction
   d. E-mail messages sent and received will be archived for not less than one year and retained in accordance with public record retention period requirements.
   e. The District may set quotas for system disk usage for individual users. The district may allow system users to increase their quota by submitting a request to the supervising teacher or system coordinator stating the need for the increase.
   f. Transmission of any materials regarding political campaigns is prohibited.
   g. Passwords may be reset or altered to applications and the District network access.
   h. Any District owned or operated computer may be re-imaged at the District's discretion.
   i. Data found to be in violation of copyright or other laws will be removed from network storage and the matter will be referred to the appropriate authority.
   j. Other conduct prohibited by the District in accordance with this policy.

8. 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.

9. Provide staff training in the appropriate use of the District network, including copies of District policy and administrative regulations. Staff will provide similar training to students.

10. Ensure all student, staff and other system users complete and sign an agreement to abide by the District's electronic communications policy and administrative regulations. Staff agreements will be maintained on file in the District office personnel files and remain in effect until policy changes

occur. Student and other user agreements will be maintained on file at each school's office and are in effect while student attends that school.

11. Determine which users will be provided access to the District network. Staff members with a current signed acceptance of the "Electronic Communications System Acceptable Use Administrative Regulation Agreement" are provided with full network and E-mail access. Students with a signed acceptance of the "Electronic Communications System Acceptable Use Administrative Regulation Agreement" will be provided Computer and Internet access and may be provided E-mail access at appropriate grade levels;

12. Cooperate fully with local, state or federal officials in any investigation relating to misuse of the District network.

System Access

Access to the District network is authorized to: Board members, District employees, students in grades K-12, with parent approval as appropriate and when under the direct supervision of staff or 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, staff, Board members, volunteers, District contractors and other members of the public may be permitted to use the District network 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 breaks and after 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 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.

General Use Prohibitions/User Responsibilities/Etiquette

Operation of the District network 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 network.

The following conduct is strictly prohibited:

1. Attempts to use the District network 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 campaigns;
    g. Facilitation of any illegal activity including "hacking"; or
    h. Cyberbullying and/or cyber-threats (see policy GBNAA/JFCFA).

2. Uploading, downloading, use, reproducing or distributing information, data, software, or file share music, videos or other materials on the District network in violation of copyright law, fair use guidelines or applicable provisions of use or license agreements.

3. Attempts to degrade, disrupt, alter with malicious intent or vandalize the District's equipment, software, materials or data or those of any other user of the District network or any of the agencies or other networks connected to the District network.

4. Use of audio and video, for noneducational purposes.

5. Use of internet and network gaming, for noneducational purposes.

6. Attempts to evade, change or exceed resource quotas or disk usage quotas.

7. Unauthorized use of District staff computers by students.

8. Sending, intentionally accessing or downloading any text file, audio file or picture or engaging in any communication that includes material which may be interpreted as:

    a. Harmful to minors;
    b. Obscene or pornographic as defined by law or indecent, vulgar, profane or lewd as determined by the District;
    c. A product or service that is illegal or not permitted to minors by law;
    d. Communication that is threatening and/or harassing, intimidating, menacing or that constitutes an expression which injures or harasses others, including cyberbullying and cyber-threats (see policy GBNAA/JFCFA);
    e. Causing a material or substantial disruption of the proper and orderly operation of the school or school activity; or
    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.

9. Attempts to gain unauthorized access via the District network to any service 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.

10. Posting or publishing student contact information on a school/District web page without building administrator approval. All such information may only be used in a manner consistent with Board policy JOA ("Directory Information"). Information subject to policy JOA includes student name, address, phone number, e-mail address, photograph, date of birth, place of birth, height and weight, dates of attendance and programs involved in.

11. Attempts by a student to arrange student meetings with anyone on the District network, unless authorized by an administrator or teacher and with prior parent approval.

12. Use of the District's name in external communication forums such as chat rooms without prior District authorization.

13. Impersonation of another user and pseudonyms, i.e., identity theft.

14. Use of another individual's account name or password to access restricted information, resources or networks to which the user has not been given access.

15. Attempts to access, copy or modify another user's files without permission.

16. Use of computers and devices connected to the District network that bypass District filtering, such as, but not limited to, cellular technology connected laptops, unless specifically authorized.

17. Attaching rogue devices or applications to District resources.

18. Remote access or remote proxy to servers or other computers outside the District network.

User Responsibilities/Etiquette:

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

System users will:

1. Adhere to the same standards for communicating online that are expected in the classroom and consistent with Board policy and administrative regulations.

2. Respect other people's time and cyberspace. Be aware of the size of any files they download and the possible effect on network performance.

3. Keep in mind that staff online practice and use of the District equipment should generally have a justifiable educational purpose. Use care even with off-hour personal shopping, surfing or games that might be misinterpreted by students or the public.

4. District-wide email messages (sent to the d7allstaff email group) should have a justifiable educational purpose and should be approved prior to dissemination by the Superintendent or designee. Items offered for sale, community notices, etc., should not be sent District-wide unless they are related to a school club or class activity. Personal items for sale and other notices can be posted on the electronic bulletin board maintained by the District for that purpose (Swap N Shop).

5. Report immediately the address of any new inappropriate site accessed accidentally by students (or staff) to the Information Services department to be added to the blocked sites.

6. Use only properly licensed software on District computers. Do not copy or share copyright-protected material without legal authorization. Installation of software not authorized by the District or included in District curriculum is prohibited.

7. Protect the integrity of the machine and/or network by not leaving their machine unattended without the use of security screen savers or other devices.

8. Protect password confidentiality. No system user should share his/her login and password with other users.

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

10. Personally owned computers (including but not limited to laptops, tablets, smart phones and other personal communication devices) may be used within the schools, when appropriate, if the operator agrees to follow all applicable use restrictions of this Policy.

Complaints

Complaints regarding use of the District network 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 appropriate disciplinary action up to and including expulsion and/or revocation of District system access.
    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 Government Standards and Practices Commission.

3. Others

    a. 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.

Telephone/Membership/Other Charges

1. 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.

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

Information Content/Third Party Supplied Information

The District makes every attempt to provide barriers to illegal and inappropriate material on the Internet and does have technology protection measures in place for all computers connected to the District network. The District cannot assure, however, that all sites which may contain material that is illegal, defamatory, obscene or potentially offensive or harmful to minors are blocked. It is ultimately all District network users who must assure the information is appropriate in accordance with district directives, and serves the educational goals and objectives of the district.

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.

The District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet. The District shall not be responsible for restoring any personally installed applications or data deemed as having no educational value. The District reserves the right to re-image any District operated computer at its discretion.

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 network 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.

Definitions

1. "Cyberbullying" is an ongoing intention by a student (or group of students) to pick on another student (or group of students) using electronic means, such as emails, instant messaging, cell phone texts, defamatory web sites, blogs, and chat rooms. This includes sending mean, vulgar or threatening messages or images; posting sensitive, private information about another person; and pretending to be someone else to make that person look bad. If an adult is involved it is called cyber-harassment or cyber-stalking and is considered criminal behavior.

2. "Cyber-threat" is online material that threatens or raises concerns about violence against others, suicide, or other self-harm. There are two kinds: direct threats and distressing material.

3. "Harmful to Minors," as defined by CIPA means any picture, image, graphic image file, sound file or other visual or audio 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.

4. "Inappropriate matter," in addition to items defined under "Harmful to Minors," any material that is inconsistent with general public education purposes, the District's mission and goals. This includes, but is not limited to, both graphic images, sound clips and text in the following categories:

    a. Weapons, violence and profanity;
    b. Full or partial nudity;
    c. Sexual acts;
    d. Gross depictions;
    e. Intolerance, intimidation, threats;
    f. Satanic or cult;
    g. Drugs/Drug culture;
    h. Militant/Extremist;
    i. Questionable activities, illegal activities and gambling;
    j. Alcohol and tobacco; and
    k. Safety/security risks.

5. "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.

6. "Sexual Act; Sexual Contact" – the terms sexual act and sexual contact have the meanings given such terms in section 2246 of Title 18, United States Code.

7. "Technology Protection Measure" – 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.

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

9. "District software" is defined as any commercial or staff developed software acquired using district resources.

Resources

Stay Safe Online, http://www.staysafeonline.org/

Embrace Civility in the Digital Age, http://www.embracecivility.org

United States Copyright Office Circular 21, Reproduction of Copyrighted Works by Educators and Librarians, http://www.copyright.gov/circs/circ21.pdf

The OR State Archivist has records retention schedules, records management training and guidelines http://arcweb.sos.state.or.us/banners/recmgmt.htm