

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

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 “D7Net” 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 “D7Net” 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, child pornography, or with respect to the use of computers by minors, 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. Grants Pass School District No. 7 has had such measures in place since the fall of 1997;
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 on-line activities of students to reduce 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;
4. 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;
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 D7Net are most applicable to the curricular needs of the District and may restrict user access, accordingly;
7. Display a message when logging into the network that reinforces key elements of the district's Electronic Communication System policy and regulation when accessed for use.
8. Set all network and application passwords to expire annually.
9. Block access to chat rooms, Internet Relay Chat and Internet E- mail sites over D7Net, except District provided E-mail & Chat Room accounts.
10. 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 D7Net are in compliance with Board policy, administrative regulations and law, the superintendent or his 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 D7Net, 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;
 - 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;
 - d. E-mail messages sent and received will be archived via district archive for up to one year. No discovery options exist past one year.
 - e. E-mail sent or received within D7Net is considered a public record and subject to state archivist rules for retention and destruction
 - f. The District may set quotas for system disk usage for individual users;
 - g. Transmission of any materials regarding political campaigns is prohibited.
 - h. Passwords may be reset or altered to applications and D7Net access.
 - i. Any District operated computer may be re-imaged at the District's discretion.
 - j. 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.
11. 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;
12. Provide staff training in the appropriate use of D7Net, including copies of District policy and administrative regulations. Staff will provide similar training to students;
13. 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.

14. Determine which users will be provided access to the D7Net. 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 under special circumstances, such as special classroom projects;
15. Cooperate fully with local, state or federal officials in any investigation relating to misuse of D7Net.

System Access

Access to D7Net 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 D7Net 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 D7Net 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 D7Net.

Prohibitions:

The following conduct is strictly prohibited:

1. Attempts to use D7Net 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; or
 - g. Instant messaging (for instance, AOL Instant Messenger);
 - h. Facilitation of any illegal activity including "hacking";
 - i. Cyberbullying and/or cyberthreats (see policy GBNA/JFCFA);

2. Uploading, downloading, use, reproducing or distributing information, data, or software, or file share music, videos or other materials on D7Net 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 D7Net or any of the agencies or other networks connected to D7Net;
4. Disruption of others' use of D7Net. Due to bandwidth constraints, the use of streaming audio and video should be limited to classroom demonstrations.
5. Use of internet radio (except for classroom use of educational content) and network gaming. They negatively affect the function of the network for all users; and are therefore specifically prohibited (except for aforementioned use of educational content);
6. Attempts to evade, change or exceed resource quotas or disk usage quotas;
7. Middle school and high school student use of any teacher computer for any reason;
8. Sending, intentionally accessing or downloading any text file, audio 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. Communication that is threatening and/or harassing, intimidating, menacing or that constitutes an expression which injures or harasses others, including cyberbullying and cyberthreats (see policy GBNA/JFCFA);
 - 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.
9. Attempts to gain unauthorized access via D7Net 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. This personal contact information is consistent with Board policy JOA ("Directory Information"). It 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 D7Net, 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. These actions are not permitted and are illegal, even if only for the purposes of "browsing".
16. Use of computers and devices 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. Use of personal communication devices for internet access that provide unfiltered connections to the Internet, thus violating the provisions of CIPA, unless specifically authorized. (see Policy JFCEB)
19. Installation and/or use of non-District authorized remote desktop or other computing utilities;
20. Remote access or remote proxy to servers or other computers outside D7Net.

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 on-line 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 affect on network performance.
3. Keep in mind that staff on-line 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 the public;
4. District-wide email messages (sent to the d7allstaff email group) should have a justifiable educational purpose. 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 not allowed;
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. System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or
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 may be used within the schools, when appropriate, if they meet the following criteria:
 - a. Must have current anti-virus software;
 - b. Provide the machine address to the District Information Systems Department;

- c. Adhere to the provisions of the District Acceptable Use Policy.
11. Remember that use of the Internet is a privilege, not a right; and inappropriate, unauthorized and/or illegal use will result in the cancellation of those privileges and appropriate disciplinary/legal action.

Complaints

Complaints regarding use of D7Net 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 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 Government Standards and Practices Commission.

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.

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 D7Net are strictly between the system user and his/her local phone company and/or long distance service provider.

School and Department Web Pages

The District encourages all schools and departments to maintain an Internet presence. It is important that the schools and the District are properly represented by information placed on the World Wide Web. Building principals and/or district administration should be aware of information published. All school and district web pages should be published on the District website, using the publishing method provided, and approved in advance by the superintendent (or designee).

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 D7Net. 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 D7Net 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. D7Net 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. **Acceptable use**-utilizing District resources (network, computing devices or applications) to satisfy educational or administrative assignments, research or tasks described wholly as official District business in the context described in the Acceptable Use Policy.
2. **Access to internet**-a computer shall be considered to have access to the Internet if such computer is connected to a computer network which has access to the Internet.

3. **Authorized account owner**-an individual authorized by the District to have access to and utilize computers/networks and/or services owned, leased or operated by the District.
4. **Child pornography**-the term child pornography shall have the meaning given such term in section 2256 of title 18, United States code.
5. **Computers/technology**-any and all computers, computer equipment, systems, hardware and/or software operated by the District. Also includes cell phones, cameras and video-cameras, PDA's and other handheld devices.
6. **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 cyberstalking and is considered criminal behavior.
7. **Cyberthreat**-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.
8. **Direct electronic communications**-any and all communications made or disseminated by electronic means, including but not limited to electronic mail, chat rooms or other forms of direct electronic communications.
9. **Fair use guidelines**-guidelines developed to clarify the application of fair use principles for educators considering digital copyright issues. (see United States Copyright Office Circular 21.)
10. **Hacking**-the act of accessing or attempting to access targeted network resources, either internal or external, for the purpose of gathering/acquiring non-privileged access and/or information, passwords, functionality, identity theft or distribution of unsolicited scripts and/or viruses.
11. **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.
12. **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;

- k. Safety/security risks;
13. **Inappropriate usage of District computers/internet/hardware & software resources**-use of the District's computers and local, intranet and internet services, that violates the District's Acceptable Use Policy or conflicts with the District's mission and purpose or with an employee's authorized job duties or responsibilities. The superintendent or his designee shall have the authority to determine what is considered to be inappropriate use.
 14. **Individuals covered by this policy**-board members, staff, students, parents and other users of computers/resource networks and/or services operated by the District.
 15. **Instant messaging**-abbreviated IM, a type of service that enables users to communicate in real time over the Internet. Typically, the IM system alerts users whenever someone from their private list is online and a chat session can be initiated with that individual.
 16. **Internet**-defined as the "standard" Internet (the collaboration and inter-connectivity of computer networks and resources worldwide) and Internet 2 (a higher educational/research form of non-commercial Internet access).
 17. **Local, Intranet and Internet computer networks**
 - a. Networks residing within the boundaries of District-owned facilities.
 - b. Leased/owned inter-connecting networks under the District's management.
 - c. Outside, non-District owned/operated networks and corresponding resources.
 18. **Minor**-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.
 19. **Obscene**-the term obscene has the meaning given such term in section 1460 of Title 18, United States Code.
 20. **Online**-active connection to network hardware, software or service resources.
 21. **Rogue access**-interpreted by the District as any connectivity to any District resources via internal network access (through devices, hard-wired drops or wireless) or external network access (Internet, Internet2, wireless, dial-in, VPN, or satellite) without notifying the District's Information Systems Department.
 22. **Rogue devices or applications**-personal hardware devices or software used/installed on the district network infrastructure or computers without notifying the Information Systems Department.
 23. **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.
 24. **Spam**-a slang term for e-mail that is the electronic equivalent of junk mail; usually advertisements, jokes or notices of no real value to the recipient.
 25. **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.
 26. **Vandalism**-any malicious attempt to harm or destroy the District's computers, data, applications, and/or network functionality or the data and/or functionality of another user's computer. This includes but is not limited to the uploading or creation of computer viruses.

27. **World Wide Web**-a collection of Internet sites that offer text and graphics and sound and animation resources through the hypertext transfer protocol and other similar protocols. It is often abbreviated “WWW” or called “the Web.”

RESOURCES:

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

The Center For Safe And Responsible Internet Use, <http://www.csriu.org/>

The Center For Safe And Responsible Internet Use’s Information On Cyberbullying, <http://cyberbully.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>

Acceptable Use Policy Student Standards

Password Protection

These guidelines are intended for use by all students using the Grants Pass School District No. 7 network. Middle and High School students will have a personal network account and an email account with a password that is assigned by the network administrators. Elementary School students will use shared network accounts; login information will be provided by their teachers as needed.

Your password allows access to applications, your class work and other files you have saved on the network. This is why password security is so critical.

Do:

- refer anyone who demands your password to the Acceptable Use Policy.
- report anyone attempting to get your username and/or password.
- inform your teacher if you suspect an account or password has been compromised
- logout when you are done using a machine you have logged into.

Don't:

- access files or applications while using another's login and password.
- write down or store a password on-line or on ANY computer system.
- share a password with anyone except your teachers, school administrators, and IS Department staff.
- use the "Remember Password" feature of applications.

Internet Safety

These guidelines are intended for use by all students who access the Internet through accounts provided by Grants Pass School District No. 7.

Do:

- use only your first name online. Unless told to do so by your teacher, don't fill out any online forms that ask for your full name, address, phone number or any other info that would help someone find you. This includes the name of your school, sports team, the town you live in, etc.
- tell your teacher if you come across any information or pictures that make you feel nervous or uncomfortable online.
- ask your teacher to notify the IS Department of any public chat rooms or other inappropriate sites that are not blocked by the web content filter.

Don't:

- send a picture of yourself or others over the Internet without your teacher's/parents' permission.
- agree to meet in person with anyone you have met on-line.
- post or do anything online that would hurt someone else. No cyber-bullying!
- post or do anything online that is against the law.
- attempt to bypass existing security and/or web filtering applications.
- download or install any software on a district computer without checking with your teacher and the Information Systems Department.

Ethical Expectations

- I will use only school appropriate language online.
- I will submit only original material that I generate, and not pretend the work of others is my own (plagiarism).
- Electronic devices such as PDA, cell phones, personally owned computers must adhere to the school policies and follow the Acceptable use regulations.
- Students bringing computers onto campus must notify the Building Administration, provide their machine's mac address, and have up to-date anti-virus software in use.
- Use of any personal electronic device for hacking, bullying, or other activities prohibited in the Acceptable Use Policy will result in confiscation of the device.

Dear Parents:

(School Name) is part of Grants Pass School District No. 7's computer-based communication network that connects all District 7 schools to each other and to the rest of the world through the Internet. Students may access this network upon written consent of a parent. The purpose of this letter is to explain the network and its services so that you will be able to decide if you wish to give permission for your student to participate in the use of this technology.

The Internet is a system which links networks creating a large and diverse communications network. It gives access to hundreds of libraries, databases and organizational web pages. With this educational opportunity also comes responsibility. It is important that you and your student read the enclosed Acceptable Use Guidelines which summarize the district Electronic Communications System Administrative Regulation and discuss these requirements together before signing the agreement form. Inappropriate system use will result in discipline up to and including expulsion from school, suspension or revocation of your student's access to D7NET and/or referral to law enforcement officials. It is our goal to prepare students for the future by providing them with an opportunity to learn how to use this global information network. All of our classrooms will have times when they are accessing information from the Internet totally teacher directed. It is important that you understand why we require your permission before your child is allowed individual access to the Internet for individual research projects.

As a class activity, Internet access will normally be supervised by a teacher; however, due to the nature of independent research and the variety of information available, the district cannot provide continual, one-on-one supervision. District and school links help direct students to appropriate sites; and we have filtering software in place that does block inappropriate material as stated in the Children's Internet Protection Act. We will monitor closely and continue to seek the most current methods to prevent student access to inappropriate materials. However, your student may inadvertently gain access that is not approved by the school district.

Although the district is committed to practices that ensure the safety and welfare of system users, including the use of technology protection measures such as Internet filtering, please be aware that there may still be material or communications on the Internet that district staff, parents and students may find objectionable. While the district neither encourages nor condones access to such material, it is not possible for us to eliminate that access completely.

Attached to this letter are the following important documents:

1. The Acceptable Use Policy Student Guidelines which summarize the district's Electronic Communications System Acceptable Use administrative regulation;
2. An agreement for your student to read and sign stating his/her agreement to follow the district's Electronic Communications System administrative regulation. This agreement requires your signature. It will remain in effect while your student is enrolled at [School Name]. If your student is in elementary school, the form requires only your signature stating you have discussed the administrative regulation with your student.

Please review these materials carefully with your student and return the attached agreement form to the [school office] indicating your permission or denial of permission for your student to participate in the district's electronic communications system.

Sincerely,
[Principal]

**Elementary School
Electronic Communications System Acceptable Use Administrative Regulation
Student Agreement**

Student agreement will remain in effect while student is enrolled at [School Name].

Student Name _____ Grade _____

School _____

Sponsoring Parent

I have read Grants Pass School District No. 7's Electronic Communications System Acceptable Use administrative regulation and discussed its provisions with my student. We understand that violation of these provisions will result in discipline up to and including expulsion from school and/or suspension or revocation of my student's access to D7NET and related privileges and/or referral to law enforcement officials.

I will monitor my student's use of the system and his/her potential access to the Internet and will accept responsibility for supervision in that regard when my student's use is not in a school setting.

In consideration for the privilege of using D7NET and in consideration for having access to the public networks, I hereby release the district, its operators and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my, or my student's use, or inability to use, the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

- _____ Yes, I give my permission for my student to use D7NET
- _____ No, I do not give my permission for my student to use D7NET

Signature of Parent _____

Home Address _____

Date _____ Home Phone Number _____

**Middle School/High School
Electronic Communications System Acceptable Use Administrative Regulation
Student Agreement**

Student agreement will remain in effect while student is enrolled at [School Name].

Student Section _____

Student Name _____ Grade _____

School _____

I have read Grants Pass School District No. 7's Electronic Communications System Acceptable Use administrative regulation and agree to abide by its provisions. I understand that violation of these provisions will result in discipline up to and including expulsion from school and/or suspension or revocation of my access to D7NET and related privileges and/or referral to law enforcement officials.

I understand that my school email account is for educational use, not social networking. I also understand that authorized school staff may access my incoming and outgoing messages.

Student Signature _____ Date _____

Sponsoring Parent

I have read Grants Pass School District No. 7's Electronic Communications System Acceptable Use administrative regulation. In consideration for the privilege of using D7NET and in consideration for having access to the public networks, I hereby release the district, its operators and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my, or my student's use, or inability to use, the system including, without limitation, the type of damages identified in the district's policy and administrative regulation.

____ Yes, I give my permission for my student to use D7NET

____ No, I do not give my permission for my student to use D7NET

Signature of Parent _____

Home Address _____

Date _____ Home Phone Number _____

Electronic Communications System Acceptable Use Administrative Regulation Agreement

(Staff and Non-Staff System User)

I agree to abide by the provisions of the Electronic Communication Acceptable Use Regulation as summarized in the included guidelines. The full Electronic Communications System Acceptable Use administrative regulation is available on the district staff web page. I understand that violation of these provisions will result in discipline up to and including dismissal in accordance with Board policy, collective bargaining agreements and applicable provisions of Federal and State law and/or referral to law enforcement officials.

I understand D7NET availability and content are on an “as-is” basis and the district makes no warranty as to its fitness for a particular purpose.

Name (please print) _____

Signature _____

School/Department _____

Certified Classified

Date _____

Acceptable Use Policy Staff Guidelines

Using School District Email Accounts

These guidelines are intended for use by all authorized account owners who access email accounts provided by Grants Pass School District No. 7.

Do:

- be very cautious when using email and do not communicate with anyone unknown to you.
- use the District's email system in a professional, ethical and legal manner.
- use the email system for educational and professional activities.
- limit personal use of email.
- immediately report any message you receive that is inappropriate or makes you feel uncomfortable.
- delete or archive old messages
- use caution with links or attachments in suspicious emails. They may spread viruses.
- remember that all District email is archived and is discoverable public record.

Don't:

- provide personal identification information (full name, home address, telephone number, etc.) about yourself or other users in email messages.
- send excessive multiple postings to people who have no interest in the content. This is known as "spamming" and is not appropriate.
- send chain letters or any unsolicited mail.
- post items for sale via email. Use the Intranet "Swap N Shop" for miscellaneous sale items.

Network Safety/Security

- Personal wireless routers are not to be installed on the District network.
- Do not install software that is not properly licensed.
- Personal laptops and computers may be used by staff within your classroom provided antivirus protection is current and mac address is registered with the Information Services Department of the machine, (personal computer equipment should be removed over break and summer).
- Donated equipment should not be accepted for classroom use unless minimum equipment requirements are met.

Acceptable Use Policy Staff Guidelines

Password Protection

These guidelines are intended for use by all authorized account owners who have been provided user accounts by Grants Pass School District No. 7. Your password allows anyone who knows it to access whatever confidential or sensitive information you have access to. This is why password security is so critical.

Do:

- create a secure password at least 6 characters long containing both letters AND numbers
- change your password to something unique as required.
- try to create passwords that can be easily remembered (but please don't use your name).
- refer anyone who demands your password to the Acceptable Use Policy.
- report anyone attempting to get your username and/or password.
- contact the I.S. Department if you suspect an account or password has been compromised.
- realize that passwords expire annually and must be changed.

Don't:

- write down or store a password on-line or on ANY computer system.
- share a password with anyone, including administrative assistants or secretaries.
- reveal a password to co-workers while on vacation.
- use the "Remember Password" feature of applications.
- reveal a password over the phone to ANYONE (except the I.S. Department).
- reveal a password in an email message
- reveal a password on questionnaires or security forms.