INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY

The Prague Public Schools district is pleased to make available to students and staff access to interconnected computer systems within the district and to the Internet, the worldwide network that provides access to significant educational materials and opportunities.

In order for the school district to ensure the continued accessibility of its computer network and the Internet, all students and staff must take responsibility for appropriate and lawful use of this access. Students and staff must understand that one person's misuse of the network and Internet access may jeopardize the ability of all students and staff to enjoy such access. While the school's teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("policy") of the school district and the Data Acquisition Site that provides Internet access to the school district. Upon reviewing, signing, and returning this policy as directed, each student and staff member agrees to follow the policy and will be given the opportunity to enjoy Internet access at school. If a student is under 18 years of age, he or she must have his or her parent or guardian read and sign the policy. The school district shall not provide access to any student who, if 18 or older, fails to sign and submit the policy to the school as directed or, if under 18, does not return the policy as directed with the signatures of the student and his/her parent or guardian.

Listed below are the provisions of the agreement regarding computer network and Internet use. The district has designated a staff member to whom users may direct questions. If any user violates this policy, the user's access will be denied or withdrawn, and the user may be subject to additional disciplinary action.

Personal Responsibility

By signing this policy, the user agrees not only to follow the rules in this policy, but also to report any misuse of the network to the person designated by the school for such reporting. Misuse means any violations of this policy or any other use that is not authorized under this policy, and having the effect of harming another or his or her property.

Term of the Permitted Use

A student or staff member who submits to the school, as directed, a properly signed policy and follows the policy to which she or he has agreed will have computer network and Internet access during the course of the school year only. Students and staff will be asked to sign a new policy each year during which they are students or staff members in the school district before they are given an access account.

Acceptable Uses

1. **Educational Purposes Only.** The school district is providing access to its computer networks and the Internet for educational purposes *only*. If the user has any doubt about whether a contemplated activity is educational, the user may consult with the person(s) designated by the school to help decide if a use is appropriate.

INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY (Cont.)

2. **Unacceptable Uses of Network.** Among the uses that are considered unacceptable and which constitute a violation of this policy are the following:

   A. Uses that violate the law or encourage others to violate the law. Do not transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the school district's student discipline policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, the user should assume that all materials are protected unless there is explicit permission on the materials to use them.

   B. Uses that cause harm to others or damage to their property. For example, do not engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than the user is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "Trojan horse," "time bomb," or other harmful form of programming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.

   C. Uses that jeopardize the security of student and staff access and of the computer network or other networks on the Internet. For example, do not disclose or share your password with others; do not impersonate another user.

   D. Uses that are commercial transactions. Students, staff, and other users may not sell or buy anything over the Internet. The user should not give others private information about the user or others, including credit card numbers and social security numbers.

3. **Netiquette.** All users must abide by rules of network etiquette, which include the following:

   A. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.

   B. Avoid language and uses that may be offensive to other users. Do not use access to make, distribute, or redistribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.

   C. Do not assume that a sender of e-mail is giving his or her permission for the user to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should be done only with permission or when the user knows that the individual would have no objection.

   D. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format that the recipient can open.

INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY (Cont.)

4. ***Cyber Bullying*** - Cyber bullying is when one or more people intentionally harm, harass, intimidate, or reject another person using technology. This includes but is not limited to the following:

   - Sending mean or threatening messages via email, IM (instant
   - messaging), or text messages.
   - Spreading rumors about others through email, IM, or text messages.
   - Creating a Web site or MySpace (or other social-networking) account that targets
   - another student or other person(s).
   - Sharing fake or embarrassing photos or videos of someone with others via a cell
   - phone or the Web.
   - Stealing another person's login and password to send mean or embarrassing messages from his or her account.

It shall be the policy of Prague Public Schools that cyber bullying will not be tolerated under any circumstances. A student caught violating this policy will lose computer privileges and these actions may result in further disciplinary action including suspension or expulsion from school of the student(s) involved. In addition, violators and their parents/guardians may be subject to civil and/or criminal penalties as specified by Oklahoma and/or federal law.

Internet Safety

1. **General Warning; Individual Responsibility of Parents and Users.** All student users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guides to materials to shun. If a student or staff member finds that other users are visiting offensive or harmful sites, he or she should report such use to the appropriate school designee.

2. **Personal Safety.** Be safe. In using the computer network and Internet, the user should not reveal personal information such as the user's home address or telephone number. The user should not use his/her real last name or any other information which might allow a person to locate the user without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone "met" on the computer network or Internet without a parent's permission (if the user is under 18). Regardless of the user's age, the user should never agree to meet a person the user has only communicated with on the Internet in a secluded place or in a private setting.

3. **"Hacking" and Other Illegal Activities.** It is a violation of this policy to use the school's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

4. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A

INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY (Cont.)

supervising teacher or administrator may authorize the release of directory information, as defined by law, for internal administrative purposes or approved educational projects and activities.

5. **Active Restriction Measures.** The school, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent users from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. We are using FortiNet for our technology protection measure (internet filtering software) to ensure that users are not accessing such depictions or any other material that is inappropriate for minors.

   Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

   The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that

   - taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

   - 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;

   - taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

6. All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

Privacy

Network and Internet access is provided as a tool for the user's education. The school district reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the school district and no user shall have any expectation of privacy regarding such materials.

Failure To Follow Policy

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the school district may refuse to reinstate for the remainder of the student's enrollment or the staff member's employment in the school district. A user violates this policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school district may also take other disciplinary action in such circumstances.

INTERNET AND OTHER COMPUTER NETWORKS ACCEPTABLE USE AND INTERNET SAFETY POLICY (Cont.)

Warranties/Indemnification

The school district makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user (or his or her parents or guardian) arising out of the user's use of its computer networks or the Internet under this policy. By signing this policy, users are taking full responsibility for their own use, and the user who is 18 or older or the parent(s) or guardian(s) of a minor student are agreeing to indemnify and hold the school, the school district, the Data Acquisition Site that provides the computer and Internet access opportunity to the school district and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or the parent(s) or guardian(s) of a minor student agree to cooperate with the school in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the school district's network.

Updates

Users, and if appropriate, their parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new policy reflecting developments in the law or technology or changes in district policy. Such information must be provided by the user (or his/her parents or guardian) or such new policy must be signed if the user wishes to continue to receive service. If after account information is provided, some or all of the information changes, the user must notify the person designated by the school to receive such information.

REFERENCE: 21 O.S. §1040.75, §1040.76
Children's Internet Protection Act of 2000 (HR 4577, P.L. 106-554)
Communications Act of 1934, as amended (47 U.S.C. 254[h], [l])
Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)

THIS POLICY REQUIRED BY LAW.