Joint School District 171 Internet Safety/Acceptable Use Agreement

Joint School District 171 makes electronic communications and Internet access available to all personnel and students. Our goal in providing this service is to promote educational excellence in schools by facilitating resource sharing, innovation and communication.

Network Etiquette—The District expects system users to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following.

- Be polite; messages typed in capital letters are equivalent to shouting and are considered rude
- Use appropriate language; do not send messages that are abusive, obscene, sexually oriented, threatening, harassing, or damaging to another's reputation
- Do not use another person's account
- Log out when you are finished using the system
- Conserve district resources related to electronic information and communications

Personal Information—Personal information consists of complete names, addresses, telephone numbers, and identifiable photos. This information is confidential when communicating on the system.

Personal Safety—No user may disclose, use, or disseminate Personal Information without authorization. Students should never reveal Personal Information without the permission of their teacher, parent, or guardian. Students should never make appointments to meet people in person, whom they have contacted on the system, without district and parent/guardian permission. Students should notify their teacher or other adult whenever they discover information or messages that they deem dangerous or inappropriate on the web, or when using electronic mail, chat rooms, or other forms of direct electronic communications.

Internet Safety—System users may not consider all materials on the Internet to be of educational value, in the context of the school setting. The District will utilize filtering software, in order to prevent system users from accessing material that is obscene, pornographic, or harmful to minors, as defined by the Children's Internet Protection Act. Users may request that a school administrator or his/her designee exclude a specific site from Internet filtering, for the purpose of bona fide research, or other educational project. The educational staff will also monitor the online activities of students through direct observation, to ensure that students do not

- Engage in inappropriate activities (chat rooms, electronic mail, and other forms of direct communication), unauthorized access (hacking) and other unlawful activities
- Disclose, use, or disseminate personal information regarding minors

Acceptable Use—Use of your network account must be in support of education and research, and consistent with the educational objectives of the school district. The District reserves the right to prioritize use and access to the system. The District prohibits transmission of any material that violates any US or State law or regulation. Forbidden items include material that is

- Copyrighted
- Threatening, pornographic, obscene, or designed to damage a person's reputation.
- Protected by a trade secret
- For commercial purposes
- Advertising for a product
- Political lobbying

The District allows limited personal use of the system, if the use

- Imposes no tangible cost to the District
- Does not unduly burden the District's computer and network resources
- Has no adverse effect on an employee's job performance
- Has no adverse effect on a student's academic performance

Vandalism—Vandalism is defined as any malicious attempt to harm or destroy district equipment or data, data of another user, this network, or other connected networks. Vandalism includes, but is not limited to, downloading, uploading or creation of computer viruses. Vandalism will result in cancellation of privileges.

Joint School District 171 Internet Safety/Acceptable Use Agreement

Security— No computer/network/email/Internet use is private. All users must use only their login or accounts, may not share their login, and shall not leave a computer open and unsupervised while they are logged in. All users shall lock (Ctrl-Alt-Del and "Lock Workstation") a computer, when leaving it unsupervised. If you feel that you can identify a security problem on the network, you must notify a system administrator; do not demonstrate the problem to others. Attempts to log on as a system administrator will result in cancellation of user privileges. Authorized personnel will review all of the District's system resources and content in the performance of their official duties (managing system resources, combating external and internal electronic attacks, etc.), and forward all forbidden items to the applicable school administrator, the superintendent, the School Board, and law enforcement personnel, as necessary. All users are responsible for all activities performed by their account; engagement in prohibited activities by district employees is grounds for dismissal.

Privileges—Use of the District's system is a privilege, not a right. Inappropriate use will result in cancellation of those privileges. All system users shall acknowledge receipt and understanding of administrative regulation governing use of the system, shall agree in writing to comply with such regulations and guidelines, and shall allow monitoring of their system use. System administrators, school administrators, directors, and the superintendent will cooperatively determine what comprises inappropriate use. System administrators may close an account at any time, in the performance of their official duties. School administration, faculty, and staff of the District may request system administrators to deny, revoke, or suspend specific user accounts.

Warranty—Joint School District 171 makes no warranties of any kind, whether expressed or implied, for the district systems. The district will not be responsible for any damages system users may suffer, with respect to any services provided by the system. This includes the loss of data resulting from delays, no deliveries, misdeliveries, or service interruptions caused by its own negligence, errors, or omissions of system users. The district does not warrant that the system will be uninterrupted or error free, or that system defects will be corrected. Use of any information obtained via the Internet is at your own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Sworn Statement

(Printed Name)

I _____ understand and will abide by the above Internet Safety/Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked; school disciplinary action may be taken; and/or appropriate legal action taken.

User's Signature: _____ Date: _____

Parent or Guardian (Must be signed if the applicant is a student and under the age of 18).

As the parent or guardian of this student, I have read the Internet Safety/Use Agreement. I understand that system access is designed for educational purposes, and that Joint School District 171 has taken precautions to secure and supervise access. However, I recognize that it is impossible for the district to restrict access to all controversial materials, and I will not hold them responsible for materials acquired on the network. Further, I accept full responsibility for supervision, if and when my children's use is not in a school setting. I hereby give permission for my child to use the Internet connections available through Joint School District 171.

Parent or Guardian's printed name: _____

Signature: _____ Date: _____

Adopted: 8/17/2009