Tri-City CUSD#1 ACCEPTABLE USE POLICY (AUP)

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. The Network is defined as all district owned hardware and software. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, (b) for legitimate school business use, or c) acceptable personal use, as defined by District Administration.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. District administration will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. Such decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
c. Using the network for private financial or commercial gain;
d. Wastefully using network resources as determined by the District;
e. Hacking or gaining unauthorized access to files, resources, or entities;
f. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;

g. Using another user's account or password;
h. Posting material authored or created by another without his/her consent;
i. Posting anonymous messages or posting messages with someone else's name on it.
j. Stealing data, equipment or intellectual property;
k. Using the network for commercial or private advertising, including solicitation or promotion of religious, and/or political activity;
l. Vandalizing, degrading or disrupting data, equipment, software, or system performance;
m. Accessing, possessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
n. Using the network while access privileges are suspended or revoked.

Consequences of violations include but are not limited to:

- Suspension of Internet/Network access.
- Revocation of Internet/Network access.
- Suspension of computer privileges.
- Revocation of computer privileges.
- Out of School suspension.
- In-school detention.
- School expulsion.
- Legal action and prosecution by the authorities.

The District has the right to restrict or terminate computer/network access at any time for any reason. The District has the right to monitor computer activity in any form that it sees fit to maintain the integrity of the computer network.

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.
b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.

d. It is the user's responsibility not to initiate access to inappropriate material. If any user accidentally or inadvertently comes in contact with questionable or inappropriate material on the network, the user should immediately exit the source and notify an appropriate staff member.
e. Recognize that electronic mail (e-mail) is not private. District administrators or their designees have access to all e-mail. Messages relating to or in support of illegal activities may be reported to the authorities. Absolute privacy cannot be guaranteed in a network environment.
f. Do not use the network in any way that would disrupt its use by other users.
g. Consider all communications and information accessible via the network to be the property of the District.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of the Acceptable Use Policy.

Security - Network security is a high priority. If the user can identify a security problem on the network, the user must notify the system administrator or building Principal immediately. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator or an unauthorized user will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, equipment, software, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Plagiarism - Plagiarism is defined in the dictionary as "taking ideas or writings from another person and offering them as your own." Credit must always be given to the person who created the article or the idea. The user, who leads readers to believe that what they are reading is the user's original work when it is not, is guilty of plagiarism. The Student Discipline Code related to plagiarism shall be applied to District computer and network use.

Copyright - According to the Copyright Act of 1976, "Fair Use" means that you may freely use any information that you legally find on the computer networks as long as you do so only for scholarly purposes. You may not plagiarize or sell what you find.

- The District reserves all rights it has under the fair use doctrine of the Copyright Act. Fair use permits limited use of copyrighted work without the author's permission for "criticism, comment, news reporting, teaching, scholarship, or research."
- Copyright laws do not protect ideas, only expression. Therefore, creative ideas posted on the District's network or Internet may be stolen with no recourse.
- All communications and information accessed via the District's computers shall be assumed to be private property of the author.

Absolute privacy cannot be guaranteed in a network environment. Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on District's servers would always be private.

Use of Electronic Mail - The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid staff

members in fulfilling their duties and responsibilities, and as an education tool.

a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
b. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.
c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
d. Any message received from an unknown sender via the Internet should either be immediately deleted or reported to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
e. Use of the School District's electronic mail system constitutes consent to these regulations.

Internet Safety – (As outlined by the Children's Internet Protection Act)

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and otherwise follow these procedures.