"COMPUTER NETWORK AND INTERNET SAFETY, ACCESS, AND USE"

I. Access to the District computer network is consistent with and beneficial to the educational mission of the District. Such access serves as a natural extension of the educational lessons learned within the classroom by providing access to educational resources and reference materials, by reinforcing the specific subject matter taught, by requiring the use of critical thinking skills, by promoting tolerance for diverse views, and by teaching socially appropriate forms of civil discourse and expression. Therefore, students shall be allowed access to the District computer network consistent with the District's curriculum, educational mission and the Acceptable Use Policy adopted by the Board of Education and outlined in the Ownership In Education manual.

II. Use of Computer Network

A. Acceptable Use

Access to the District computer network must be for bona fide educational or research purposes consistent with the District's educational mission. Access also must comply with the Policy, Computer Network and Internet Safety, Access and Use Policy, these Rules and Regulations, other rules, regulations or other terms or conditions of computer network access **(complete text of policy is available from the ASC, Building Principal, or District Website)** and all other disciplinary policies and regulations necessary for the safety and educational concerns of the District.

B. Unacceptable Use

Any use which disrupts the proper and orderly operation and discipline of schools in the District; threatens the integrity or efficient operation of the District computer network; violates the rights of others; is socially inappropriate or inappropriate for a student's age or maturity level; is primarily intended as an immediate solicitation of funds; is illegal or for illegal purposes of any kind; or constitutes gross disobedience or misconduct is an unacceptable use. Use of the District computer network for any unacceptable use will result in the suspension or revocation of computer network privileges, disciplinary action, and/or appropriate legal action.

Unacceptable uses of the District's computer network specifically include, **but are not limited to**, the following:

1. Taking any steps which threaten, or which may reasonably be interpreted to threaten, any person, group of persons, building, or property with harm, regardless of whether the user intends to carry out such threat;

2. Compromising the privacy or safety of other individuals by disclosing personal addresses, telephone numbers, or other personal identifying information;

3. Accessing, using or possessing any material in a manner that constitutes or furthers fraud (including academic fraud), libel, slander, plagiarism, forgery, or a violation of copyright or other intellectual property right;

4. Using the computer network for commercial, private, or personal financial gain, including gambling;

5. Deliberately accessing, creating, displaying, transmitting, or otherwise possessing or disseminating material which contains pornography, obscenity, or sexually explicit, pervasively lewd and vulgar, or indecent or inappropriate language, text, sounds, or visual depictions;

6. Creating or forwarding chain letters, "spam," or other unsolicited or unwanted messages;

7. Creating or sending e-mail or other communications which purport to come from another individual (commonly known as "spoofing"), or otherwise assuming an anonymous or false identity in communicating with other individuals, businesses, or organizations;

8. Modifying, disabling, compromising, or otherwise circumventing any anti-virus, user authentication, or other security feature maintained on the District network or on any external computer, computer system, or computer account;

9. Using or accessing another user's computer network account or password, with or without consent from that user;

10. Disclosing any computer network password (including your own) to any other individual;

11. Downloading or installing text files, images, or other files or software to the District's computer network without prior permission from the Superintendent, Building Principal, or their designees;

12. Creating or deliberately downloading, uploading, or forwarding any computer virus, or otherwise attempting to modify, destroy, or corrupt computer files maintained by any individual on any computer;

13. Participating in, or subscribing to, mailing lists, newsgroups, chat services, electronic bulletin boards, or any other association or service which would cause a large number of e-mails or other electronic messages to be sent to the District's computer network;

14. Using encryption software or otherwise encoding or password-protecting any file which is created with, sent to, received by, or stored on the District's computer network;

15. Attempting to commit any action which would constitute an unacceptable use if accomplished successfully.

III. Enforcement

The failure of any user to abide by the Policy, these Rules and Regulations, or other rules, regulations or other terms or conditions of computer network access adopted by the Board of Education will result in the suspension or revocation of the user's computer network privileges, disciplinary action, and/or appropriate legal action. Computer network privileges may be suspended or revoked by the Superintendent or Building Principal. Disciplinary measures, if any, will be considered and imposed consistent with District discipline policies.