APPENDIX VII

INTERNET SAFETY AND ACCEPTABLE USE POLICY

District: Greenville Public Schools
Section: I – Instructional Program
Policy: IJBA – Internet Safety & Acceptable Use Policy

Policy:

Greenville Public School District Internet Safety and Acceptable Use Policy

With the spread of telecommunications throughout society, including the educational environment, the Greenville Public School District Board recognizes that students and employees will shift the way they access and transmit information, share ideas, and communicate with others. As schools and offices are connected to the global community, the use of new tools and technologies brings new responsibilities as well as opportunities. Network resources are intended for educational purposes and to carry out the legitimate business of the school district. The Greenville Public School District Board expects all users of the district's computing and network resources, including electronic mail and telecommunications tools, to utilize these resources appropriately.

It is the policy of the Greenville Public School District to:

a) prevent user access over its computer network to, or transmission of, inappropriate material via internet, electronic mail, or other forms of direct electronic communications;
b) prevent unauthorized access and other unlawful online activity;
c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors; and
d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Greenville Public School District to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information Technology Department.

The Instructional Technology Department will provide age-appropriate training for students who use the District's Internet facilities. The training provided will be designed to promote the District's commitment to:
The standards and acceptable use of Internet services as set forth in the District's Internet Safety Policy;

Student safety with regard to: safety on the Internet; appropriate behavior while online, on social networking websites, and in chat rooms; and cyber-bullying awareness and response.
Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "internet filters") shall be used to block or filter internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of materials deemed obscene or pornographic, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for *bona fide* research or other lawful purposes.''

Section I: DEFINITIONS

A. Child Pornography
The term "child pornography" has the meaning given such term in § 2256 of Title 18, United States Code.

B. Harmful to Minors
The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC § 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.

C. Minor
The term "minor" means an individual who has not attained the age of 17.

D. Obscene
The term "obscene" has the meaning given such term in § 1460 of Title 18, United States Code.

E. Sexual Act; Sexual Contact

The terms "sexual act" and "sexual contact" have the meanings given such terms in § 2246 of Title 18, United States Code.

F. Directory Information

The term "directory information" is defined by the Family Educational Rights and Privacy Act Regulations (20 USC §1232g; 34 CFR Part99) as information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended.

Section II: ACCEPTABLE USE

Acceptable Uses of Network

The Greenville Public School District is providing access to its computer networks and the internet only for educational purposes or to carry out the legitimate business of the school district.

Unacceptable Uses of Network

Among the uses that are considered unacceptable and which constitute a violation of this policy are, but are not limited to, the following:

Uses that violate the law or encourage others to violate the law

Examples include: transmitting offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by the district's Student Code of Conduct; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials.

Uses that cause harm to others or damage to their property

Examples include: engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the internet; uploading a worm, virus, or other harmful form of programming or vandalism; participating in hacking activities or any form of unauthorized access to other computers, networks, or information systems.

Uses that jeopardize the security of user access and of the computer network or other networks on the internet

Examples include: disclosing or sharing your password with others; impersonating another user.

Uses that are commercial or political in nature

Examples include: using the network for personal financial gain or profit; using the network to give others private information about yourself or others, including credit card numbers and social security numbers.

Uses that cause harm to the district's computer, network, or equipment

Examples include: installing software programs, instant programs, altering system settings, or otherwise reconfiguring computers without approval of the appropriate personnel.

Uses that are inconsistent with the purpose of the network and internet

Examples include: using internet games, chat rooms, and instant messaging not specifically assigned by a teacher or administrator; downloading music or video files or any other files that are not directly related to a school assignment.

NETIQUETTE

All users must abide by rules of network etiquette, which include the following:

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

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

Do not assume that a sender of an email is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her email address to third parties.

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

Section III: INTERNET SAFETY

General Warning

All users, and the parents/guardians of minor users, are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his/her use of the computer network and internet and stay away from these sites. If a student finds that other users are visiting offensive or harmful sites, he/she should report such use to the person designated by the school.

Personal Safety

Be safe. In using the computer network and internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. If you are a minor, do not arrange a face-to-face meeting with someone you "meet" on the computer network or internet without your parent's permission. Regardless of your age, you should never agree to meet a person you have only communicated with on the internet in a secluded place or in a private setting.

Hacking and Other Illegal Activities

It is a violation of this policy to use the district'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.

Confidentiality of Student Information

Personal identifiable information concerning minor students may not be disclosed or used in any way on the internet without the permission of a parent or guardian, or for non-minors, without the person's consent. Users should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers.

The schools or district may authorize the release of directory information, as defined by the Family Educational Rights and Privacy Act (FERPA) for internal administrative purposes, approved.

"Cyber-Bullying" includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another person by sending or posting

inappropriate and hurtful email messages, instant messages, text messages, or posting inappropriate and hurtful email messages, instant messages, text messages, digital pictures or images, or website postings, including blogs through the District's computer network and the internet, whether accessed on campus or off campus, during or after school hours. In the situation that cyber-bullying originated from a non-school computer, but brought to the attention of school officials, any disciplinary actions shall be based on whether the conduct is determined to be disruptive of the educational environment or a detriment to students and/or staff. Administration may, in its discretion, contact law enforcement or other appropriate authorities.

Section J Students
Policy Code: JDDA- Bullying

The Greenville Public School District does not discriminate on the basis of race, color, creed, sex, religion, or national origin.