4526.1 INTERNET SAFETY POLICY

INTRODUCTION

It is the policy of the 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 information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA") [Pub. L. No. 106-554 and 47 USC § 254(h)]. It is the goal of this policy not only to prevent and protect, but to educate employees, students, parents and the community in Internet safety. The CIPA guidelines for an Internet Safety Policy have also been incorporated by the School District into its Acceptable Use Policies.

The Children's Internet Protection Act, enacted December 21, 2000, requires recipients of federal technology funds to comply with certain Internet filtering and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connection services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities.

This policy is intended to be read together with the School District's Acceptable Use Policies for Technology and the Internet as applicable to School District employees and students. All limitations and penalties set forth in the Acceptable Use Policies are deemed to be incorporated into this policy. Terms used in this policy which also appear in the Children's Internet Protection Act have the meanings defined in the Children's Internet Protection Act.

COMPLIANCE WITH THE REQUIREMENTS OF CIPA:

Technology Protection Measures Technology Protection Measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, involve child pornography, or are harmful to minors. In addition to the filtering system that is incorporated with the Internet service provided by Southern Westchester BOCES, the School District subscribes to a content filtering system, on all computers that access the Internet, which is compliant with CIPA and NCIPA.

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 and textual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

The district utilizes Marshal 8e6 R3000 internet filter gateway and Barracuda Spam Filtering for Email. This software protects against access by adults and minors to visual depictions that are obscene, child pornography, or with respect to use of computers with Internet access by minors harmful to minors. The software may be disabled for adults engaged in bona fide research or other lawful purposes. Any attempt to bypass, defeat or circumvent the Technology Prevention Measures is punishable as a violation of this policy and of the Acceptable Use Policies.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the School District's online computer network when using electronic mail, chat rooms, blogging, instant messaging, online discussions and other forms of direct electronic communications. Without limiting the foregoing, access to such means of communication is strictly limited by the Acceptable Use Policies.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring

It shall be the responsibility of all professional employees (pedagogical and administrative staff) of the School District to supervise and monitor usage of the School District's computers, computer network and access to the Internet in accordance with this policy, the Acceptable Use Policies, and the Children's Internet Protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Technology or designated representatives.

Education

The School District will advocate and educate employees, students, parents and the community on Internet safety and "cyber-bullying." Education will be provided through such means as professional development training and materials to employees;

PTO presentations; and community outreach opportunities such as: local public access television and School District websites.

Cyber-bullying

The Acceptable Use Policies include provisions intended to prohibit and establish penalties for inappropriate and oppressive conduct, including cyber-bullying.

The School District is a place of tolerance and good manners. Students may not use the network or any School District computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability is prohibited. Network users may not use vulgar, derogatory, or obscene language. Network users may not post anonymous messages or forge e-mail or other messages.

Furthermore, School District computers and network facilities may not be used for any activity, or to transmit any material, that violates United States, New York State or local laws. This includes, but is not limited to any threat or act of intimidation or harassment against another person.

Adoption date: June 16, 2010