Operations Policy #915.1
Children's Internet Protection Act (CIPA)

Background:
According to the Pennsylvania Department of Education (PDE), the Federal Children's Internet Protection Act "(CIPA)", Pub. L. No. 106-554 and 47 USC 254(h), mandates that schools that receive federal technology funds must develop and implement measures and policies to prevent access to "visual depictions" that are determined to be "obscene", "child pornography", or "harmful to minors" as defined herein.

PDE has further stated that schools receiving certain E-rate discounts are also mandated by the Neighborhood Children's Internet Protection Act (N-CIPA) to adopt and enforce an Internet Safety Policy (ISP) that addresses harmful or inappropriate online activities. N-CIPA was passed as part of CIPA.

Purpose:
The Board of Trustees of SusQ-Cyber Charter School ("SusQ-Cyber") has adopted this Policy in order to establish specific standards to comply with CIPA and N-CIPA requirements.

Guidelines:
- This Policy is to be read in conjunction with the SusQ-Cyber's Internet Acceptable Use Policy and shall supplement, not supplant, SusQ-Cyber's Internet Acceptable Use Policy.

- The Chief Executive Officer "CEO" or his/her designee is directed to include this Policy in the Parent and Student Handbook and the Employee Handbook. Failure to comply with this Policy and/or Internet safety requirements of SusQ-Cyber shall result in consequences as set forth in the school's Parent and Student handbook, Code of Conduct or Employee Handbook and/or as allowed by applicable law. Consequences may include, but are not limited to: denial of or restriction to access to technology, suspension, expulsion, notification of authorities, termination, commencement of civil and/or criminal proceedings and/or other consequences available under school policy and/or applicable state and/or federal laws.
- This Policy has been adopted after reasonable public notice and at a meeting held open to the public to address this policy.

Purpose
SusQ-Cyber uses computer resources to facilitate the education of students and to aid in matters related to the operations of SusQ-Cyber. SusQ-Cyber further places student Internet safety as a primary concern.

It is every computer user's duty to use computer resources, including the Internet, responsibly, professionally, ethically and lawfully. Access to these resources shall be designated a privilege, not a right.

This policy applies to aspects of both adult and student compliance with Internet safety at SusQ-Cyber.

Adopted 2/17/15

CIPA/N-CIPA Compliance/Internet Safety

It is the policy of SusQ-Cyber to:

1. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, and all other forms of direct electronic communications;
2. Prevent unauthorized access and other unlawful online activity;
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. Comply with the Children's Internet Protection Act, Pub. L. No. 106-554 and 47 USC 254(h).

To the extent consistent with applicable state and federal laws and reasonably practical, technology protection measures (or "Internet filters") shall be used at SusQ-Cyber to block or filter Internet, and other forms of electronic communications, and access to inappropriate information. The form and type of technology protection measures used during the 2009-2010 school year include: BESS and Gaggle.

The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of title 18, United States Code;
2. Child Pornography, as that term is defined in section 2256 of Title 18, United States Code; or
3. Harmful to minors. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
    a) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
    b) 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; and
    c) Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

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

As required by the Children's Internet Protection Act (CIPA), blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Technology protection measures shall only be disabled pursuant to the direction of the CEO or his designee to the extent allowed by applicable law and regulation, for bona fide research or other lawful purposes of an adult as determined by the CEO or his/her designee. The

development of procedures for the disabling or otherwise modifying of any technology protection measures shall be the responsibility of the CEO of SusQ-Cyber or his designee.

Delegation of Responsibility:

The CEO or his/her designee shall take reasonable steps to promote the safety and security of users of the online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

As required by the Children's Internet Protection Act, prevention of inappropriate network usage at SusQ-Cyber shall include:

1) Unauthorized access, including so-called 'hacking', and other unlawful activities; and
2) Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

It shall be the responsibility of all members of the SusQ-Cyber staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and applicable laws, including the Children's Internet Protection Act as well as in accordance with any administrative procedures developed by the CEO in furtherance of this Policy.

In accordance with the "Protecting Children in the 21st Century Act" and its requirement to certify to the Schools and Library Division ("SLD") that the school's Internet Safety Policy includes educating minors about appropriate online behavior, students shall be educated about appropriate online behavior, including cyber-bullying awareness and response and interacting with other individuals on social networking sites and in chat rooms.

With regard to educating minors about appropriate online behavior, the CEO or his /her designee is directed to:

1) Make such educational opportunities available to students during the school year;
2) Notify students and their parents about these educational opportunities in advance; and
3) Maintain documentation of:
    a) educational programs offered;
    b) the dates and locations of such opportunities
    c) how online safety was taught and what was covered in the programs offered; and
    d) those in attendance at the programs offered.

The CEO or his designee is directed to file and/or provide the appropriate certifications evidencing compliance with CIPA and N-CIPA as required by applicable state and/or federal laws and regulations.

The CEO or his/her designee is directed to maintain documentation of compliance with CIPA and N-CIPA certification requirements including the annual filing of FCC Form 486.

The CEO or his/her designee is directed to ensure that SusQ-Cyber employs necessary technology protection measures in accordance with this Policy and shall report to the Board when modifications are needed to technology protection measures at SusQ-Cyber.

The online activities of students shall be monitored and minors' access to harmful materials shall be restricted to the extent required by applicable laws and regulations.
To the extent not inconsistent with applicable laws and regulations, the following disclaimers apply:

1) There shall be no expectation of privacy by users of SusQ-Cyber's Computer Resources;
2) SusQ-Cyber does not guarantee the effectiveness of technology protection measurers or internet filtering; and
3) SusQ-Cyber does not guarantee network functionality or accuracy of online information.

The CEO is directed to implement any procedures that may be necessary to implement this policy as well as to timely submit any forms and paperwork as required by CIPA and N-CIPA and/or applicable state and federal Internet safety laws and regulations.

TO THE EXTENT THAT ANYTHING IN THIS POLICY COULD BE CONSTRUED TO CONFLICT WITH APPLICABLE STATE AND/OR FEDERAL LAWS, THE APPLICABLE STATE AND/OR FEDERAL LAWS CONTROL. THIS POLICY IS NOT INTENDED TO CONFLICT WITH CHARTER REQUIREMENT.

Adopted 2/17/15