INTERNET SAFETY PLAN

The Sussex County Charter School for Technology has technology protection measures for all computers in the school that block and/or filter visual depictions that are obscene, child pornography and harmful to minors as defined in the Children's Internet Protection Act. The school will certify that it is in compliance with the Children's Internet Protection Act and acceptable use regulations of the school.

Compliance measures contained within this plan address the following:

Access by Minors to Inappropriate Matter on the Internet and World Wide Web

1. Users will not use the network system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, special exception may be made for hate literature if the purpose of such access is to conduct research AND access is approved by both the teacher and the parent. School employees may access the above material only in the context of legitimate research.

2. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner set for by the school. Students should immediately notify teachers. Teachers and staff should immediately notify building administration. Building administration should immediately notify the technology coordinator. This will protect users against an allegation that they have intentionally violated the acceptable use policy.

3. The fact that the filtering software has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the filtering software has protected access to certain material shall not create the presumption that the material is inappropriate for users to access.

4. The board will provide student access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain.

Safety and Security of Minors when using Electronic Mail, Chat Rooms, and other Forms of Direct Electronic Communications and Unauthorized Disclosures

1. Student users will not post or share contact information about themselves or other people. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent's name, home address or location, work address or location, or phone number.

2. Students will not disclose their full name or any other personal contact information for any purpose.

3. Students will not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. Students will not forward a message that was sent to them privately without permission of the person who sent them the message.

5. Students will not agree to meet someone they have met online.

6. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

Unauthorized Access, Including "Hacking" and other Unlawful Activities by Minors Online

1. Security on any computer network is a high priority, especially when the network involves many users. If a user feels that he/she can identify a security problem on the computer network, the user must notify a network administrator or an administrator. The user should not inform individuals other than the network administrators or administrators of a security problem.

2. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.

3. Passwords to the network should not be easily guessable by others, nor should they be words that could be found in a dictionary.

4. Attempts to log in to the network using either another user's account or as a network administrator could result in termination of the account. Users should immediately notify the network administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk will have limitations placed on usage of the network or may be terminated as a user and be subject to other disciplinary action.

5. Users will not attempt to gain unauthorized access to the school system or to any other computer system through the school system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing".

6. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

7. Users will not use the district system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

Technology Protection Measure (Software Filtering)

The school has a technology protection measure (software filtering) for use with the school's Internet system. The filtering software will always be configured to protect against access material that is obscene, child pornography and material that is harmful to minors, as defined by the Children's Internet Protection Act. The district or individual schools may, from time to time, reconfigure the filtering software to best meet the educational needs of the school and address the safety needs of the students.

The technology coordinator will conduct an annual analysis of the effectiveness of the selected filter and will make recommendations to the Chief School Officer regarding the selection and configuration of the filter.

The filter may not be disabled at any time that students may be using the district Internet system, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The filter may be disabled during non-student use time for system administrative purposes.

Filtering software has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains school control over decision making regarding the appropriateness of material for students, does not unduly restrict the educational use of the school Internet system by teachers and students, and ensures the protection students' constitutional right to access to information and ideas, authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the filter.

Authority to temporarily unblock access will be granted to administrators and or his/her designees, and any media specialists or teacher who regularly uses the Internet for instructional purposes who request permission to have such authority. Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are deemed necessary to ensure the security of the system. The technology coorindator shall determine such standards.

To temporarily unblock a site, the authorized individual must review the content of the site, outside of the presence of any student, prior to allowing access to the site by a student.

Reports of all instances of temporary unblocking will automatically be forwarded to the technology coordinator.

If an unauthorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forward to the technology coordinator. He/She will make a decision to permanently unblock access to the site or may delegate the decision to the school administration. A list of all sites that have been permanently unblocked, together with the rationale for making the decision to unblock the site will be forwarded on a monthly basis to the chief administrator.

Notwithstanding the visual depictions defined in the Children's Internet Protection Act and as defined in this Plan, and Acceptable Use Policy and Regulation of Acceptable Use Policy, the board shall determine Internet material that is inappropriate for minors. The board will provide reasonable public notice and will hold one annual public hearing to address and receive public community input on this Internet Safety Plan, and Acceptable Use Policy and Regulation of Acceptable Use Policy.

Notice of the annual public hearing will be generated through school publications and will be posted on the district web site.

....More on the Technology Protection Measure Utilized by

The Children's Internet Protection Act (CIPA) became law on April 20, 2001. To be in compliance with this legislation, public school districts must certify that they have measures in place that block or filter Internet access for both minors and adults to certain visual depictions.

The Sussex County Charter School for Technology uses Internet content filtering software by K12USA called "secureschool" which blocks access to web sites flagged as potentially-offensive by K12USA currently one of the nation's largest databases of blocked sites. The filtering platform itself is operated off-site, and is updated from N2H2's managed list on a daily basis.

The N2H2 service works in a similar way to programs such as CYBERsitter, Cyber Patrol, and Net-Nanny, however it is designed to efficiently service "server-based" filtering. With server-based solutions, a site is blocked before it gets to the user's computer. It has proven to be an efficient, cost effective, and reliable filtering solution.