

## **INTERNET SAFETY POLICY**

The purpose of the Internet is to facilitate communications in support of research and education, by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user, the use of District Computer Network (Network) accounts must be in support of and consistent with the educational objectives of the district. Guidelines for use are practical and logical extensions of our district's commitment to legal, responsible, ethical, and considerate (thoughtfully respectful of others) usage of the Internet.

Because the Internet is a fluid environment, the information which will be available to students is constantly changing; therefore, it is impossible to predict with certainty what information students might locate. Just as the purchase, availability, and use of media materials does not indicate endorsement of their contents by school officials, neither does making electronic information available to students imply endorsement of that content.

### **The Children's Internet Protection Act: Internet Content Filtering/ Safety Policy**

In compliance with The Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the Catskill School District has adopted and will enforce this Internet policy that ensures the use of technology protection measures (i.e. filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to the Internet access of both adults and minors to visual depictions that are obscene, child pornography, to the use of computers by minors, or considered harmful to such students. Further, appropriate monitoring of online activities of minors, as determined by the building administrator, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the District's Board of Education's decision to utilize technology measures and other safety procedures, for staff, students, and authorized guests when accessing the Internet fosters the educational mission of the District including selection of appropriate teaching/ instructional materials and activities too enhance the District's programs; and to help ensure the safety of staff and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the Network Administrator, will be provided to ensure compliance with the CIPA.

**INTERNET SAFETY POLICY**

(Continued)

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web may include, but shall not be limited to, the following activities:

- Ensuring the presence of a teacher and/or other appropriate school personnel when students are accessing the Internet and/or other forms of electronic communications. As designated by the superintendent, the use of the Internet may be blocked as deemed necessary to ensure the safety of such students;
- Lists of student user accounts and passwords to the network and filter access logs are maintained by the Network Administrator. Access to these lists is available to school personnel.
- Lists of student computer and/or Internet permission forms are to be entered electronically into the student information system by the Administrator's designee and kept on file in the main office. New student's computer and/or Internet permission forms are to be entered electronically into the student information system by the Central Registrar. Student forms should be then sent to the appropriate school's main office for filing. Access to these lists is available to school personnel.
- The dissemination of the District's Information Technology Use Policy and accompanying Regulations to parents and students in order to provide notice of the District's requirements, expectations, and students consent, as may be applicable, shall be required prior to authorization for student use of the District's computers. In compliance with the Internet Safety Policy, as well as the District's Information Technology Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies will result in disciplinary action.

**INTERNET SAFETY POLICY**

(Continued)

It is the intention of the Catskill Central School District Board of Education to:

- Ensure that students will not have access to inappropriate materials when using the District Computer Network, Internet or e-mail, and other forms of direct electronic communications such as video conferencing, distance learning, and shadowing via Thin Client, etc.
- Prevent unauthorized access and other unlawful activities by users of the District's Computer Network
- Prevent unauthorized disclosure, use dissemination of personal identification information regarding users; and comply with all federal and state regulations.

**Definitions**

The following definitions apply to this policy:

Inappropriate Materials: Any material that is obscene, child pornography, or harmful to minors.

Child Pornography: Any visual depiction which involves the use of a minor engaging in sexually explicit conduct; or where a depiction appears to be of a minor or has been created, adapted, or modified to appear that a minor is engaging in such conduct; is advertised, promoted, presented, described or distributed in a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

Harmful to Minors: 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, and 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.

**INTERNET SAFETY POLICY**

(Continued)

Obscene: Any material or performance when, considered as a whole, predominately appeals to a prurient interest in sex; or that depicts or describes in a patently offensive manner actual or simulated sexual acts, sexual contact, nudity, sadism, masochism, excretion, or a lewd exhibition of the genitals and that lacks serious literary, artistic, political, or scientific value.

Technology Protection Measures: Specific technology that blocks or filters Internet access.

**Prevention of Access to Inappropriate Materials on the Internet**

In accordance with the Children's Internet Protection Act, the Board authorizes the Superintendent of Schools to have technology protection measures installed on the District Computer Network to block or filter access to the internet, e-mails, chat rooms, and other forms of direct electronic communication by the students, staff, and authorized guests using the District Computer Network,. The District has installed an Internet Filtering Service technology to provide the following safety features:

1. Safety for all computer users - to prevent access to inappropriate materials.
2. Protect Confidential Information - to prevent unauthorized disclosure, use and dissemination of personal identification information regarding minors and school personnel.
3. Prevent Unauthorized Access - to prevent unauthorized access, including "hacking" and other unlawful activities on the Network and Internet. Student violations of such policies will result in disciplinary action.

Teachers and administrators are allowed to request ad hoc adjustments to the filter to make available appropriate sites with legitimate educational value initially blocked by the filter and to block inappropriate sites not blocked by the filter.

**Privacy and Safety on the District's Web Site**

At no time shall any student's personal information (home address, e-mail address, phone numbers, names of family members and friends) appear on the District's web site or link sites.

At no time shall any teacher's or other staff member's personal information (home address, e-mail address, phone numbers, names of family members and friends) appear on the District's web site or linked sites without the permission of the individual.

**INTERNET SAFETY POLICY**

(Continued)

**Information on Adults**

Information on adults which is widely held to be public information (such as the names of members of the Board of Education and district offices) may be published on the web site as needed. Information on adults, which is not public information, may be published ONLY with the expressed permission of the individual.

**Information on Minors Younger Than 13**

NO information on minors younger than 13, which could be used to identify any particular individual, is to be published on the District web site or any site to which the District web site links. Forbidden content includes names (first and/or last) and identifiable photographs.

**Information on Minors between the Ages of 13 and 18**

Limited information on minors between the ages 13 and 18 (such as their names, photographs and projects) may be published on the web site ONLY with the expressed WRITTEN permission of the minor's custodial parent or guardian. The school should keep a copy of the completed permission form and send the original to the District Web Site Coordinator along with the material being submitted. If any parent or guardian revokes permission after the photographs have been published on the web site, any photographs in which that child was included will be removed from the website.

**Information on Minors Younger Than 13**

NO information on minors younger than 13, which could be used to identify any particular individual, is to be published on the District web site or any site to which the District web site links. Forbidden content includes names (first and/or last) and identifiable photographs without parent permission.

**INTERNET SAFETY POLICY**

(Continued)

**Publishing Photographs**

Group and individual photographs may be published on the District websites with WRITTEN permission. No names may be used to identify students without prior WRITTEN permission obtained from the minor's custodial parent or guardian and they are to be informed that permission is being obtained so that the photographs may be published on the website. If any parent or guardian revokes permission after the photographs have been published on the website, any photographs in which that child was included will be removed from the website.

Cross Ref: 4526.1 Information Technology Use Policy for Students

4526.2 District Web Site Policy

4526.2-R District Website Regulation

Revised: July 19, 2007

Adoption date: September 26, 2007