

*Existing mandated policy and regulation, adopted/approved 5/20/14, appropriate as written, with CABE samples to review and compare. The requirement on filtering is also covered in Woodbridge's existing policy and regulation #6141.321. Please review to combine.*

## **Instruction**

### **Internet Acceptable Use: Filtering**

The Woodbridge School District is fortunate to have access to the Internet. This access provides increased opportunities for students and staff to conduct research and to communicate locally, nationally, and internationally.

The Board of education provides computers, computer systems, software, electronic access and networks for students and staff to carry out the mission of the Board in an environment which ensures access to up-to-date information, management, and communication services. Responsible use of these systems and networks is expected of all students and staff.

The computers, computer systems, software, electronic access and networks are the property of the Board of Education and are to be used only for those activities directly related to teaching, learning, and/or management by students and staff. The equipment, infrastructure, and software are provided exclusively for school related use. The system may be used for personal communications only to a limited extent, which does not interfere with the statutes and/or other policies governing employment of the District.

In order to ensure that the District's Internet connection is used in the appropriate manner and that all user are protected from any inappropriate information published on the Internet, the District has and is continuing to implement the following:

1. Professional development opportunities to help teachers integrate the use of the Internet into classroom teaching.
2. Use of the computers, computer systems, software, electronic access, and networks shall be restricted to those users who have signed the District's "Acceptable Use Policy." In the case of minors, the "Acceptable Use Policy" must also be signed by the student's parent or guardian.
3. In compliance with this policy, a system to filter out Internet sites.

Filtering should only be viewed as one of a number of techniques use to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to inappropriate material. Filtering should be used in conjunction with:

- Educating students to be safe and responsible users of electronic communications and resources.
- Using recognized Internet gateways as a searching tool and/or homepage for students in order to facilitate access to appropriate material.
- Using "Acceptable Use Policy Agreements."
- Appropriate supervision, both in person and electronically.

## **Instruction**

### **Internet Acceptable Use: Filtering (continued)**

The placement of filters on District computers/computer systems is viewed as an exercise of the Board's ability to determine educational suitability of all material used in the schools.

Filters may be utilized to (1) block pre-selected site, (2) block by content, (3) block entire categories like chat and newsgroups and (4) allow a pre-selected list of approved sites.

The District recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response.

(cf. 5148 – Electronic Information/Technology/Media)

(cf. 6141.321 – Acceptable Use of the Internet)

(cf. 6141.322 – Web Sites/Pages)

Legal Reference:      Connecticut General Statutes  
                                 1-19(b)(11) Access to public records. Exempt records.  
                                 10-15b Access of parent or guardians to student's records.  
                                 10-209 Records not to be public.  
                                 11-8a Retention, destruction and transfer of documents  
                                 11-8b Transfer or disposal of public records. State Library Board to adopt regulations.  
                                 46b-56 (e) Access to Records of Minors.  
                                 Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).  
                                 Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C. 1232g.).  
                                 Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.  
                                 Public Law 106-554 Fiscal 2001 Appropriations Law containing the "Children's Internet Protection Act"  
                                 Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.  
                                 Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21<sup>st</sup> Century Act  
                                 *Reno v. ACLU*, 521 U.S. 844 (1997)  
                                 *Ginsberg v. New York*, 390 U.S. 629, at 642, n.10 (1968)  
                                 *Board of Education v. Pico*, 457 U.S. 868 (1988)  
                                 *Hazelwood School District v. Kuhlmeier*, 484 U.S. 620, 267 (1988)

Policy adopted:      May 20, 2014

WOODBIDGE PUBLIC SCHOOLS  
Woodbridge, Connecticut

*Existing regulation approved 5/20/14, also covered in existing 6141.321, review to combine.*

## **Instruction**

### **Internet Acceptable Use: Filtering**

#### **Preface**

When minors are using the Internet, access to visual depictions that are obscene, child pornography or harmful to minors must be blocked or filtered. When adults are using the Internet, only material which is obscene or child pornography must be filtered or blocked.

#### **Definitions**

**1. Obscene** is to be determined by the following test:

- Whether the average person, applying contemporary community standards, would find the work, taken as a whole, appeals to the prurient interest;
- Whether the work depicts sexual conduct in a patently offensive way; and
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

**1. Child Pornography**, as defined in 18 U.S.C. 2256 means any visual depiction, including any photograph, film, video, picture, computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
- such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
- such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

**1. Material “Harmful to Minors”** is any picture, 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 to minors, an actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

## **Instruction**

### **Internet Acceptable Use: Filtering (continued)**

#### **Criteria for Filtering of Objectionable Sites**

Anything that falls under at least one of the categories below shall be blocked/filtered. This list will be updated/modified as required.

#### **Nudity/Pornography**

- Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
- Provocative semi-nudity (e.g., lingerie models)
- Sites which contain pornography or links to pornographic sites
- **Exceptions:** Classical nudity (e.g., Michelangelo), swimsuit models

#### **Sexuality**

- Sites which contain material of a mature level (elementary/middle school levels)
- Images or descriptions of sexual aids
- Descriptions of sexual acts or techniques
- Sites which contain inappropriate personal ads

#### **Violence**

- Sites which promote violence
- Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
- Graphic autopsy or crime-scene images

#### **Crime**

- Information of performing criminal acts (e.g., drug or bomb making, computer “hacking”)
- Illegal file archives (e.g., software piracy)

#### **Drug Use**

- Sites which promote the use of illegal drugs
- Material advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
- **Exceptions:** Material with valid educational use (e.g., drug-use statistics)

#### **Tastelessness**

- Images or descriptions of excretory acts (e.g., vomiting, urinating)
- Graphic medical images outside of a medical context
- **Exception:** Graphic medical images within a medical context

## **Instruction**

### **Internet Acceptable Use: Filtering**

#### **Criteria for Filtering of Objectionable Sites (continued)**

##### **Language/Profanity**

- Passages/Words too coarse to be softened by the word filter
- Profanity within images/sounds/multimedia files
- Adult humor (e.g., sexually or racially tinged)

**Note:** The focus is on American English, but profanity in other languages or dialects is blocked if brought to our attention.

##### **Discrimination/Intolerance**

- Material advocating discrimination (e.g., racial or religious intolerance)
- Sites which promote intolerance, hate, or discrimination

##### **Interactive Mail/Chat**

- Sites which contain or allow inappropriate e-mail correspondence
- Sites which contain or allow inappropriate chat areas

##### **Inappropriate Banner Acts**

- Advertisements containing inappropriate images

##### **Gambling**

- Sites which allow or promote online gambling

##### **Weapons**

- Sites which promote illegal weapons
- Sites which promote the use of illegal weapons

##### **Other Inappropriate Material**

- \* Body modification: tattooing, branding, cutting, etc.

##### **Judgment Calls**

- Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

## **Instruction**

### **Internet Acceptable Use: Filtering (continued)**

#### **Procedures for Suggesting Site be Blocked or Unblocked**

If District staff members observe a site which they believe to contain inappropriate material according to the criteria provided here, they may request that the site (URL) be blocked. Education Technology staff will review the site for inappropriateness. If the site meets the criteria for filtering, steps will be taken to block the site.

#### **Disabling Blocking/Filtering Devices**

The technology protection measures used to block or filter a site may/may not be disabled during use by an adult to enable access to bona fide research or other lawful purpose.

*A Mandated policy to consider. The Children's Internet Protection Act (CIPA) requires that schools and libraries receiving E-Rate discounts for Internet access, service or internal connections, must block or filter all access to visual depictions that are obscene, child pornography, harmful to minors, or that is determined by the school district or library authority as inappropriate to minors.*

## **Instruction**

### **Internet Responsible Use: Filtering**

The \_\_\_\_\_ Public Schools is fortunate to have access to the Internet at all schools. This access provides increased opportunities for students and staff to conduct research and to communicate locally, nationally, and internationally.

This wonderful resource also provides access to material unsuitable for students and which has no educational value. It is the responsibility of all District staff to ensure that the Internet, as used in District Schools, is appropriately guided and monitored. Moreover, staff also has the responsibility to conduct themselves in an appropriate private manner when using the Internet.

#### **Alternative/optional language to consider**

*The Board of Education provides computers, computer systems, software, electronic access privileges, and networks for students and staff to carry out the mission of the Board in an environment which ensures access to up-to-date information, management, and communication services. Responsible use of these systems and networks is expected of all students and staff.*

*The computers, computer systems, software, electronic access privileges, and networks are the property of the Board of Education and are to be used only for those activities directly related to teaching, learning, and/or management by students and staff. The equipment, infrastructure, and software are not to be used for personal gain by any student or staff member.*

In order to ensure that the District's Internet connection is used in the appropriate manner and that all users are protected from any inappropriate information published on the Internet, the District has and is continuing to implement the following:

1. Professional development opportunities to help teachers integrate the use of the Internet into classroom teaching.
2. Use of the computers, computer systems, software electronic access privileges and networks shall be restricted to those users who have signed the District's "Responsible Use Policy." In the case of minors, the "Responsible Use Policy" must also be signed by the student's parent or guardian.
3. Implementation of a system developed to filter out Internet sites with content/material considered inappropriate or harmful and unacceptable for student viewing. Such content includes that which is considered obscene, child pornography or harmful to minors. A committee of teachers, parents, and administrators shall be used to receive appeals from users who indicate that they have a specific need for using a filtered site.

## Instruction

### Internet Responsible Use: Filtering (continued)

4. All Internet access must be filtered, whether minors (under 18) or adults are using the computer system and regardless of the number of computers with Internet access provided by the school or library.

The Internet changes rapidly making it impossible to filter all objectionable sites. Therefore, the staff role in supervising and monitoring student access to the Internet is critical. In addition, each individual has the responsibility to monitor their own navigation on the Internet to avoid undesirable sites.

#### Alternative/optional language to consider

*Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage Responsible usage. It should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors. Filtering should be used in conjunction with:*

- *Educating students to be "Net-smart;"*
- *Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material;*
- *Using "Responsible Use Agreements;"*
- *Using behavior management practices for which Internet access privileges can be earned or lost; and*
- *Appropriate supervision, either in person and/or electronically.*

*The placement of filters on District computers/computer systems is viewed as an exercise of the Board's ability to determine educational suitability of all material used in the schools.*

*Filters will be utilized with District schools to (1) block pre-selected sites, (2) block by word, (3) block entire categories like chat and newsgroups, and (4) through a pre-selected list of approved sites.*

*The Superintendent of Schools is directed to establish guidelines and procedures for responsible use of computers, computer systems, software, electronic access privileges, and networks provided by the Board of Education.*

*For districts participating in the federal E-Rate program:*

The District recognizes its responsibility to educate students regarding appropriate behavior on social networking and chat room sites about cyberbullying. Therefore, students shall be provided instruction about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyberbullying awareness and response."



## Instruction

### Internet Responsible Use: Filtering (continued)

(cf. 6141.321 - Responsible Use of the Internet)

(cf. 6141.322 - Web Sites/Pages)

Legal Reference: Connecticut General Statutes  
1-19(b)(11) Access to public records. Exempt records.  
10-15b Access of parent or guardians to student's records.  
10-209 Records not to be public.  
11-8a Retention, destruction and transfer of documents  
11-8b Transfer or disposal of public records. State Library Board to adopt regulations.  
46b-56 (e) Access to Records of Minors.  
Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).  
Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C. 1232g.).  
Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.  
Public Law 106-554 Fiscal 2001 Appropriations Law containing the "Children's Internet Protection Act"  
Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.  
Public Law 110-385 Broadband Data Improvement Act/Protecting Children in the 21<sup>st</sup> Century Act  
*Reno v. ACLU*, 521 U.S. 844 (1997)  
*Ginsberg v. New York*, 390 U.S. 629, at 642, n.10 (1968)  
*Board of Education v. Pico*, 457 U.S. 868 (1988)  
*Hazelwood School District v. Kuhlmeier*, 484 U.S. 620, 267 (1988)

Policy adopted:

cps 7/01  
rev 1/09  
rev 5/24

*A sample regulation to consider.*

## Instruction

### Internet Responsible Use: Filtering

#### Preface

When minors are using the Internet, access to visual depictions that are obscene, child pornography or harmful to minors must be blocked or filtered. When adults are using the Internet, only material which is obscene or child pornography must be filtered or blocked.

#### Definitions

2. **Obscene** is to be determined by the following test:

- Whether the average person, applying contemporary community standards, would find the work, taken as a whole, appeals to the prurient interest;
- Whether the work depicts sexual conduct in a patently offensive way; and
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

2. **Child Pornography**, as defined in 18 U.S.C. 2256 means any visual depiction, including any photograph, film, video, picture, computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct;
- such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or
- such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

2. Material **“Harmful to Minors”** is any picture, 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 to minors, an actual or simulated sexual act or sexual conduct, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Criteria for Filtering of Objectionable Sites**

Anything that falls under at least one of the categories below shall be blocked/filtered. This list will be updated/modified as required.

#### **Nudity/Pornography**

- Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
- Provocative semi-nudity (e.g., lingerie models)
- Sites which contain pornography or links to pornographic sites
- **Exceptions:** Classical nudity (e.g., Michelangelo), swimsuit models

#### **Sexuality**

- Sites which contain material of a mature level (elementary/middle school levels)
- Images or descriptions of sexual aids
- Descriptions of sexual acts or techniques
- Sites which contain inappropriate personal ads

#### **Violence**

- Sites which promote violence
- Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
- Graphic autopsy or crime-scene images

#### **Crime**

- Information of performing criminal acts (e.g., drug or bomb making, computer “hacking”)
- Illegal file archives (e.g., software piracy)

#### **Drug Use**

- Sites which promote the use of illegal drugs
- Material advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
- **Exceptions:** Material with valid educational use (e.g., drug-use statistics)

#### **Tastelessness**

- Images or descriptions of excretory acts (e.g., vomiting, urinating)
- Graphic medical images outside of a medical context
- **Exception:** Graphic medical images within a medical context

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Criteria for Filtering of Objectionable Sites (continued)**

##### **Language/Profanity**

- Passages/Words too coarse to be softened by the word filter
- Profanity within images/sounds/multimedia files
- Adult humor (e.g., sexually or racially tinged)

NOTE: The focus is on American English, but profanity in other languages or dialects is blocked if brought to our attention.

##### **Discrimination/Intolerance**

- Material advocating discrimination (e.g., racial or religious intolerance)
- Sites which promote intolerance, hate, or discrimination

##### **Interactive Mail/Chat**

- Sites which contain or allow inappropriate e-mail correspondence
- Sites which contain or allow inappropriate chat areas

##### **Inappropriate Banner Acts**

- Advertisements containing inappropriate images

##### **Gambling**

- Sites which allow or promote online gambling

##### **Weapons**

- Sites which promote illegal weapons
- Sites which promote the use of illegal weapons

##### **Other Inappropriate Material**

- \* Body modification: tattooing, branding, cutting, etc.

##### **Judgment Calls**

- Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Procedures For Suggesting Site Be Blocked or Unblocked**

If District staff members observe a site which they believe to contain inappropriate material according to the criteria provided here, they may request that the site (URL) be blocked. Education Technology staff will review the site for inappropriateness. If the site meets the criteria for filtering, steps will be taken to block the site.

#### **Disabling Blocking/Filtering Devices**

The technology protection measures used to block or filter a site may/may not be disabled during use by an adult to enable access to bona fide research or other lawful purpose. (*NOTE: CIPA does not require schools or libraries to afford adults unfiltered Internet access.*)

There are no exceptions to the requirement that Internet access be blocked/filtered at all times for minors. If material has been wrongly blocked, it must be unblocked by the company providing the software, after a request has been made by the school or library.

Regulation approved:

cps 7/01

cps 5/24

*Another sample policy to consider.*

*This version accomplishes the requirements of CIPA by requiring the required elements of the legislation be addressed in the administrative regulations for the policy rather than in policy language. This approach is consistent with the principle that detailed requirements are more appropriately handled in administrative regulations authorized by board policy.*

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Access to Electronic Networks**

Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation and communication. The Superintendent or his/her designee shall develop an administrative regulation containing an implementation plan for this policy. The implementation plan shall include, but not be limited to, integration of the Internet in the curriculum, staff training, software filters and safety issues.

The District is not responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved or transmitted via the Internet. In addition, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

#### **Curriculum**

The use of the District's electronic networks shall:

1. be consistent with the curriculum adopted by the Board of Education as well as the varied instructional needs, learning styles, abilities and developmental levels of the students, and
2. comply with the selection criteria for instructional materials and library-media center materials.

Staff members may, consistent with the Superintendent's regulations and implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

*NOTE: School authorities may reasonably regulate student expression in school-sponsored publications for educationally related reasons. This policy allows such control by stating that the school-sponsored network is not a "public forum" open for general student use, but is a part of the curriculum.*

#### **Responsible Use**

All use of the District's electronic network must be:

1. in support of education and/or research and be in furtherance of the Board of Education's goals, or
2. for a legitimate school business purpose.

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Responsible Use (continued)**

Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted or received via the District's electronic network or computers. General rules for behavior and communications apply when using electronic networks as contained in Board policy #6141.321, "Responsible Use of the Internet." Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

#### **Internet Safety**

Each district computer with Internet access shall have a filtering device that blocks entry to visual depictions that are obscene, pornographic or harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee. The Superintendent or his/her designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or his/her designee.

*NOTE: The policy's provision for prior approval is not in the law and may be omitted. The entire sentence may be deleted if the Board does not want the filtering device to be disabled.*

The Superintendent or his/her designee shall include measures in this policy's implementation plan and administrative regulation to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including "hacking" and other unlawful activities; and
4. Limiting unauthorized disclosure, use and dissemination of personal identification information.

#### **Authorization for Electronic Network Access**

Each student and his/her parent or guardian must sign the District's authorization form prior to being granted unsupervised use of the network. Staff members must also sign the form as a condition of use.

## Instruction

### Internet Responsible Use: Filtering

#### Authorization for Electronic Network Access (continued)

All users of the District's computers and means of Internet access shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is placed onto the network.

The failure of any student or staff member to follow the terms of the authorization form, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

(cf. 6141.321 - Responsible Use of the Internet)

(cf. 6141.322 - Web Sites/Pages)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

11-8a Retention, destruction and transfer of documents

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

46b-56 (e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C. 1232g.).

Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

Public Law 106-554 Fiscal 2001 Appropriations Law containing the "Children's Internet Protection Act"

Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.

*Reno v. ACLU*, 521 U.S. 844 (1997)

*Ginsberg v. New York*, 390 U.S. 629, at 642, n.10 (1968)

*Board of Education v. Pico*, 457 U.S. 868 (1988)

*Hazelwood School District v. Kuhlmeier*, 484 U.S. 620, 267 (1988)

Policy adopted:

cps 7/01

rev 5/24



*A shortened version to consider.*

## **Instruction**

### **Internet Responsible Use: Filtering**

The Board of Education has:

- a responsibility to enable students to utilize the Internet and participate in the increasingly information-based society of today;
- a responsibility to enable students to cope with the wide-range and volume of material available through the Internet; and
- a duty of care to protect their students from excessively inappropriate material on the Internet for the students' age group.

Therefore, the Board directs the Superintendent to implement a system designed to filter out Internet sites containing visual depictions that are obscene, pornographic or harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee. The Superintendent or his/her designee shall enforce the use, at all times, of such filtering devices. This filtering system shall be in addition to all other efforts utilized to help ensure student access to approved educational materials.

(cf. 6141.321 - Responsible Use of the Internet)

(cf. 6141.322 - Web Sites/Pages)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

11-8a Retention, destruction and transfer of documents

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

46b-56 (e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

## **Instruction**

### **Internet Responsible Use: Filtering**

Legal Reference: (continued)

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C.1232g.).

Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.

Public Law 106-554 Fiscal 2001 Appropriations Law containing the “Children’s Internet Protection Act”

*Reno v. ACLU*, 521 U.S. 844 (1997)

*Ginsberg v. New York*, 390 U.S. 629, at 642, n.10 (1968)

*Board of Education v. Pico*, 457 U.S. 868 (1988)

*Hazelwood School District v. Kuhlmeier*, 484 U.S. 620, 267 (1988)

Policy adopted:

cps 7/01  
rev 5/24

*An administrative regulation to consider  
if this is not presently in the District's administrative regulation,  
#6141.321, pertaining to "Responsible Use of the Internet."*

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Responsible Use of Electronic Networks**

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, communication and appropriate behavior. These procedures do not attempt to state all required or prescribed behavior by users. However, some specific examples are provided.

#### **Terms and Conditions**

- 1. Responsible Use** – Students and staff are responsible for maintaining appropriate ethical and behavioral standards when using technology.
- 2. Privileges** - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The administration will make all decisions regarding whether or not a user has violated ethical or behavioral standards and may deny, revoke, or suspend access at any time; his or her decision is final.
- 3. Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
  - a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law;
  - b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
  - c. Downloading copyrighted material for other than personal use;
  - d. Using the network for private financial or commercial gain;
  - e. Wastefully using resources, such as file space;
  - f. Hacking or gaining unauthorized access to files, resources, or entities;
  - g. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;
  - h. Using another user's account or password;
  - i. Posting material authorized or created by another without his/her consent;
  - j. Posting anonymous messages;

## Instruction

### Internet Responsible Use: Filtering

#### Responsible Use of Electronic Networks (continued)

#### Terms and Conditions (continued)

- k. Using the network for commercial or private advertising;
  - l. Accessing, submitting, posting, publishing, or displaying a defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
  - m. Using the network while access privileges are suspended or revoked.
4. **Etiquette** - The user is expected to abide by the generally accepted rules of behavioral etiquette. These include, but are not limited to, the following:
- a. Be polite. Do not become abusive in messages to others.
  - b. Use appropriate language.
  - c. Do be responsible of privacy and the security of others.
  - d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
  - e. Consider all communications and information accessible via the network to be private property.
5. **No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. **Indemnification** - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.
7. **Security** - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

## Instruction

### Internet Responsible Use: Filtering

#### Responsible Use of Electronic Networks (continued)

#### Terms and Conditions (continued)

7. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
9. **Charges** - The District assumes no responsibility for any unauthorized charges or fees.
10. **Copyright Web Publishing Rules** - Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.
  - a. For each republication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
  - b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of “public domain” documents must be provided.
  - c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
  - d. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
  - e. Student work may only be published if there is written permission from both the parent/guardian and student.
11. **Use of Electronic Mail**
  - a. The District’s electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
  - b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
  - c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Responsible Use of Electronic Networks (continued)**

#### **Terms and Conditions (continued)**

- d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- f. Use of the School District's electronic mail system constitutes consent to these regulations.

### **Internet Safety**

- 1. Internet access is limited to only those "responsible uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and otherwise follow these procedures.
- 2. Staff members shall monitor student use while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet Access contained in these procedures.
- 3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.
- 4. The system administrator and Building Principals shall monitor student Internet access.

Legal Reference: Children's Internet Protection Act, P.L. 106-554.  
20 U.S.C § 6801 et seq.  
47 U.S.C. § 254(h) and (1).  
720ILCS 135/0.01.

Regulation approved:

cps 7/01  
rev 5/24

## Instruction

### Internet Responsible Use: Filtering

### Responsible Use of Electronic Networks

#### Authorization for Electronic Network Access

*Each staff member must sign this Authorization as a condition for using the District's Electronic Network connection. Each student and his or her parent(s)/guardian(s) must sign the Authorization before being granted unsupervised access. Please read this document carefully before signing.*

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization does not attempt to state all required or prescribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the Authorization for Electronic Network Access will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

#### Terms and Conditions

1. **Responsible Use** – Students and staff are responsible for maintaining appropriate ethical and behavioral standards when using technology.
2. **Privileges** - The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has this Authorization and may deny, revoke, or suspend access at any time; his or her decision is final.
3. **Unacceptable Use** - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
  - a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law;
  - b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-licensed;
  - c. Downloading copyrighted material for other than personal use;
  - d. Using the network for private financial or commercial gain;
  - e. Wastefully using resources, such as file space;
  - f. Hacking or gaining unauthorized access to files, resources, or entities;
  - g. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;
  - h. Using another user's account or password;
  - i. Posting material authorized or created by another without his/her consent;
  - j. Posting anonymous messages;

## Instruction

### Internet Responsible Use: Filtering

### Responsible Use of Electronic Networks

#### Terms and Conditions (continued)

- k. Using the network for commercial or private advertising;
  - l. Accessing, submitting, posting, publishing, or displaying a defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
  - m. Using the network while access privileges are suspended or revoked.
4. **Etiquette** - The user is expected to abide by the generally accepted rules of behavioral etiquette. These include, but are not limited to, the following:
- a. Be polite. Do not become abusive in messages to others.
  - b. Use appropriate language.
  - c. Do be responsible of privacy and the security of others.
  - d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
  - e. Consider all communications and information accessible via the network to be private property.
5. **No Warranties** - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. **Indemnification** - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Authorization.
7. **Security** - Network security is a high priority. If you can identify a security problem on the Internet, you must notify the System Administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.



## Instruction

### Internet Responsible Use: Filtering

### Responsible Use of Electronic Networks

#### Terms and Conditions (continued)

8. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
9. **Charges** - The District assumes no responsibility for any unauthorized charges or fees.
10. **Copyright Web Publishing Rules** - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.
  - a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
  - b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
  - c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
  - d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
  - e. Student work may only be published if there is written permission from both the parent/guardian and student.
11. **Use of Electronic Mail**
  - a. The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
  - b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
  - c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

## **Instruction**

### **Internet Responsible Use: Filtering**

### **Responsible Use of Electronic Networks**

#### **Terms and Conditions** (continued)

#### **11. Use of Electronic Mail** (continued)

- a. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- b. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- c. Use of the School District's electronic mail system constitutes consent to these regulations.

#### **Internet Safety**

1. Internet access is limited to only those "responsible uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in this Authorization, and otherwise follow this Authorization.
2. Staff members shall monitor student use while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this Authorization.
3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.
4. The system administrator and Building Principals shall monitor student Internet access.

Students, parent(s)/guardian(s), and staff members need only sign this *Authorization for Electronic Network Access* once while enrolled or employed by the School District.

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my E-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Internet.

DATE: \_\_\_\_\_

USER SIGNATURE: \_\_\_\_\_

*(Required if the user is a student:)*

I have read this *Authorization for Electronic Network Access*. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this Authorization with my child. I hereby request that my child be allowed access to the District's Internet.

DATE: \_\_\_\_\_

PARENT/GUARDIAN NAME (Please Print): \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

*A form letter which addresses the issue of filtering.*

\_\_\_\_\_  
\_\_\_\_\_  
**Public Schools  
, Connecticut**

Dear Parent/Guardian:

The \_\_\_\_\_ Public Schools is fortunate to have a connection to the Internet to supplement the other resources already available to staff and students. Through the Internet, your child will have the entire world at his or her fingertips and be able to explore it.

This wonderful resource brings with it added responsibility. As Internet users, we must be aware of the many issues that surround the Internet. There are many valuable resources available on the Internet that may not be found elsewhere. At the same time there are many sites that can be considered inappropriate for students and serve no educational value. It is the responsibility of all users, staff and students alike, to ensure that, at all times while in a \_\_\_\_\_ Public School, the Internet is being used only for educational purposes. Student use of the Internet is being used only for educational purposes. Student use of the Internet will be under the supervision of \_\_\_\_\_ Public School staff.

The attached "Responsible Use Policy" should be read carefully and understood by all Internet users. As parents/guardians, you should review it in detail with your children before they begin using the Internet in their classroom. The "Responsible Use Policy" strives to ensure the safety of all users. A filtering system designed to prevent access to certain unacceptable sites is being installed to help eliminate this problem. However, it is important to understand that no solution is perfect and we cannot guarantee that students will only have access to educational materials.

It is important that you and your children understand that any violation of the "Responsible Use Policy" will result in the loss of Internet privileges or other disciplinary action. We ask that you work with your children in reinforcing the behaviors associated with the "Responsible Use Policy."

Thank you for your support of this important new opportunity for \_\_\_\_\_ Public School students.

Sincerely,

\_\_\_\_\_  
Principal

*A sample regulation to consider.*

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Criteria for Filtering of Objectionable Sites**

Anything that falls under at least one of the categories below shall be blocked. This list may be updated/modified as required.

##### **Nudity/Pornography**

- Prevailing U.S. standards for nudity (e.g., genitalia, female breasts)
- Provocative semi-nudity (e.g. lingerie models)
- Sites which contain pornography or links to pornographic sites
- **Exceptions:** Classical nudity (e.g., Michelangelo)

##### **Sexuality**

- Sites which contain material of a mature level (elementary/middle school levels)
- Images or descriptions of sexual aids
- Descriptions of sexual acts or techniques
- Sites which contain inappropriate personal ads

##### **Violence**

- Sites which promote violence
- Images or a description of graphically violent acts (rape, dismemberment, torture, etc.)
- Graphic autopsy or crime-scene images

##### **Crime**

- Information of performing criminal acts (e.g., drug or bomb making, computer “hacking”)
- Illegal file archives (e.g., software piracy)

##### **Drug Use**

- Sites which promote the use of illegal drugs
- Material advocating the use of illegal drugs (e.g., marijuana, LSD) or abuse of any drug (e.g., drinking-game rules)
- **Exceptions:** Material with valid educational use (e.g., drug-use statistics)

##### **Tastelessness**

- Images or descriptions of excretory acts (e.g., vomiting, urinating)
- Graphic medical images outside of a medical context
- **Exception:** Graphic medical images within a medical context

##### **Language/Profanity**

- Passages/Words too coarse to be softened by the word filter
- Profanity within images/sounds/multimedia files
- Adult humor (e.g., sexually or racially tinged)

NOTE: The focus is on American English, but profanity in other languages or dialects is blocked if brought to our attention.

## **Instruction**

### **Internet Responsible Use: Filtering**

#### **Criteria for Filtering of Objectionable Sites (continued)**

##### **Discrimination/Intolerance**

- Material advocating discrimination (e.g., racial or religious intolerance)
- Sites which promote intolerance, hate, or discrimination

##### **Interactive Mail/Chat**

- Sites which contain or allow inappropriate e-mail correspondence
- Sites which contain or allow inappropriate chat areas

##### **Inappropriate Banner Acts**

- Advertisements containing inappropriate images

##### **Gambling**

- Sites which allow or promote online gambling

##### **Weapons**

- Sites which promote illegal weapons
- Sites which promote the use of illegal weapons

##### **Other Inappropriate Material**

- Body modification: tattooing, branding, cutting, etc.

##### **Judgment Calls**

- Whether a page is likely to have more questionable material in the future (e.g., sites under construction whose names indicate questionable material)

#### **Procedures for suggesting site be blocked or unblocked**

If District staff members observe a site which they believe to contain inappropriate material according to the criteria provided here, they may request that the site (URL) be blocked. Education Technology staff will review the site for inappropriateness. After consulting with the Administrative staff, if the site meets the criteria for filtering, steps will be taken to block the site.

Regulation approved:

cps 4/01

rev 5/24

*A shortened version to consider.*

## **Instruction**

### **Internet Responsible Use: Filtering**

The Board of Education has

- a responsibility to enable students to utilize the Internet and participate in the increasingly information-based society of today;
- a responsibility to enable students to cope with the wide-range and volume of material available through the Internet; and
- a duty of care to protect their students from excessively inappropriate material on the Internet for the students' age group.

Therefore, the Board directs the Superintendent to implement a system designed to filter out Internet sites with content considered unacceptable and inappropriate for student viewing. This filtering system shall be in addition to all other efforts utilized to help ensure student access to approved educational materials.

(cf. 6141.321 - Technology and Instruction)

(cf. 6141.322 - WebSites/Pages)

(cf. 6141.321 - Responsible Use of the Internet)

(cf. 6141.322 - Web Sites/Pages)

Legal Reference: Connecticut General Statutes

1-19(b)(11) Access to public records. Exempt records.

10-15b Access of parent or guardians to student's records.

10-209 Records not to be public.

11-8a Retention, destruction and transfer of documents

11-8b Transfer or disposal of public records. State Library Board to adopt regulations.

46b-56 (e) Access to Records of Minors.

Connecticut Public Records Administration Schedule V - Disposition of Education Records (Revised 1983).

Federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, as amended, added by section 513 of PL 93-568, codified at 20 U.S.C.1232g.).

Dept. of Education. 34 CFR. Part 99 (May 9, 1980 45 FR 30802) regs. implementing FERPA enacted as part of 438 of General Education Provisions Act (20 U.S.C. 1232g)-parent and student privacy and other rights with respect to educational records, as amended 11/21/96.

## **Instruction**

### **Internet Responsible Use: Filtering**

Legal Reference (continued)

Public Law 94-553, The Copyright Act of 1976, 17 U.S.C. 101 et. seq.

HR 4577, Fiscal 2001 Appropriations Law )contains Children's Internet Protection Act)

*Reno v. ACLU*, 521 U.S. 844 (1997)

*Ginsberg v. New York*, 390 U.S. 629, at 642, n.10 (1968)

*Board of Education v. Pico*, 457 U.S. 868 (1988)

*Hazelwood School District v. Kuhlmeier*, 484 U.S. 620, 267 (1988)

Regulation approved:

cps 4/01

rev 5/24