Board Office Use: **Legislative File Info.**	
File ID Number	14-0813
Introduction Date	5-14-14
Enactment Number	14-0745
Enactment Date	5/14/14

OAKLAND UNIFIED SCHOOL DISTRICT

Community Schools, Thriving Students

Memo

To Board of Education

From Maria Santos, Deputy Superintendent
John Krull, Information Technology Officer Executive Officer Technology Services

Board Meeting Date May 14, 2014

Subject Amendments to Board Policy 6163.4 and Administrative Regulation 6163.4 Student Use of Technology

---

Action Requested Approval of modifications in Board Policy 6163.4 and Administrative Regulation 6163.4 Student Use of Technology

Background The District's existing Board Policy relating to student's use of technology sets forth the Board's expectations for student's use of technology to ensure that such use is consistent with the Board's policies and the applicable laws relating to student safety, anti-discrimination, prohibition against cyberbullying, and protection of personal information of students while recognizing the important role of technology in advancement of student learning.

Discussion The modifications to the Board Policy last updated in 2012 refine terminology and are needed due to advances in the way students use technology throughout the District The modifications to the Administrative Regulation which was last updated in 2004 align with the California Schools Boards Association model regulation and provide for training of staff on requirements regarding student use of technology and staff role in supervising student use of technological resources, add categories of prohibited conduct to further prevent improper use of technological resources and clarify the consequences for inappropriate use of technology.

The modifications have been reviewed and vetted by the General Counsel.
The changes to the policy are shown on the attachment.

Recommendation Approval of the modifications to Board Policy 6163.4 Student Use of Technology and Administrative Regulation 6163.4.

Fiscal Impact N/A

Attachments Board Policy 6163.4 with proposed changes to existing Board Policy 6163.4 in redline format; the Proposed Board Policy 6163.4 in final format (without redlines); Administrative Regulation 6163.4 with proposed changes to existing Administrative Regulation 6163.4 in redline format; the Proposed Administrative Regulation 6163.4 in final format (without redlines)

OAKLAND UNIFIED SCHOOL DISTRICT
Administrative Regulation

AR 6163.4
Instruction

Student Use of Technology

The principal or designee shall oversee the maintenance of each school's technological resources while following District standards set by the Technology Services department and may establish guidelines and limits on their use. Instructional staff shall receive a copy of this administrative regulation, the accompanying Board policy, and the district's Acceptable Use Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All students using these resources shall receive training in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 4040 - Employee Use of Technology)
(cf. 4131- Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)
(cf. 6162.7 - Use of Technology in Instruction)

At the beginning of each school year, parents/guardians shall receive a copy of the district's policy and administrative regulation regarding access by students to the Internet and on-line sites. (Education Code 48980)

(cf. 5145.6 - Parental Notifications)

On-Line/Internet Services: User Obligations and Responsibilities

Students are authorized to use district equipment to access the Internet or on-line services in accordance with user obligations and responsibilities specified below and in accordance with Governing Board policy and the district's Acceptable Use Agreement.

1. The student, in whose name an on-line services account is issued, is responsible for its proper use at all times. Students shall keep personal account numbers, passwords, home addresses and telephone numbers private. They shall only use the system under their own account to which they have been assigned.

2. Students shall use the district's system safely, responsibly and primarily for educational purposes.

3. Students shall not access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as

harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

(cf. 5145.3 - Nondiscrimination/Harassment)
(cf. 5145.7 - Sexual Harassment)
(cf. 5145.9 - Hate-Motivated Behavior)

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes in a patently offensive way sexual conduct and which lacks serious literary, artistic, political or scientific value for minors. (Penal Code 313)

4. Students shall not disclose, use or disseminate personal identification information about themselves or others when using electronic mail, chat rooms, or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals located through the Internet without the permission of their parents/guardians.

Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.

5. Students shall not use the system to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or Board policy. If a user violates the Acceptable Use Agreement or any of the District's or a school's policies, regulations procedures or guidelines, access to the District's educational technology resources may be denied and other legal or disciplinary action may be taken.

(cf. 3513.3 - Tobacco-Free Schools)

6. Students shall not use the system to engage in commercial or other for-profit activities.

7. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.

8. Copyrighted material shall not be placed on the system without the author's permission and in accordance with copyright laws. Students may download copyrighted material for their own use only and with proper credit given, as with any other printed source of information.

(cf. 5131.9 Academic Honesty
cf. 6162.6 - Use of Copyrighted Materials)

9. Students shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

(cf. 5131.5 - Vandalism, Theft and Graffiti)

10. Students shall not read or use other users' electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify or forge other users' mail.

11. Students shall report any security problem or misuse of the services to the teacher or principal.

The district reserves the right to monitor the use of the district's system for improper use without advance notice or consent. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by district officials to ensure proper use of the system.

(cf. 5145.12 - Search and Seizure)

Whenever a student is found to have violated Board policy, administrative regulation, or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

7/14/04;4/14A

OAKLAND UNIFIED SCHOOL DISTRICT
Administrative Regulation

AR 6163.4
Instruction

Student Use of Technology

The principal or designee shall oversee the maintenance of each school's technological resources while following District standards set by the Technology Services department and may establish guidelines and limits on their use. Instructional staff shall receive a copy of this administrative regulation, the accompanying Board policy, and the district's Acceptable Use Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. ~~He/she shall ensure that a~~All students using these resources shall receive training in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 4040 - Employee Use of Technology)
(cf. 4131- Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)
(cf. 6162.7 - Use of Technology in Instruction)

At the beginning of each school year, parents/guardians shall receive a copy of the district's policy and administrative regulation regarding access by students to the Internet and on-line sites. (Education Code 48980)

(cf. 5145.6 - Parental Notifications)

On-Line/Internet Services: User Obligations and Responsibilities

Students are authorized to use district equipment to access the Internet or on-line services in accordance with user obligations and responsibilities specified below and in accordance with Governing Board policy and the district's Acceptable Use Agreement.

1. The student, in whose name an on-line services account is issued, is responsible for its proper use at all times. Students shall keep personal account numbers, passwords, home addresses and telephone numbers private. They shall only use the system ~~only~~ under their own account to which they have been assigned ~~number~~.

2. Students shall use the district's system safely, responsibly and primarily for educational purposes.

3. Students shall not access, post, submit, publish or display harmful or inappropriate matter

that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

(cf. 5145.3 - Nondiscrimination/Harassment)
(cf. 5145.7 - Sexual Harassment)
(cf. 5145.9 - Hate-Motivated Behavior)

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes in a patently offensive way sexual conduct and which lacks serious literary, artistic, political or scientific value for minors. (Penal Code 313)

4. Students shall not disclose, use or disseminate personal identification information about themselves or others when using electronic mail, chat rooms, or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals located through the Internet without the permission of their parents/guardians.

Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.

5. Students shall not use the system to encourage the use of drugs, alcohol or tobacco, nor shall they promote unethical practices or any activity prohibited by law or Board policy. If a user violates the Acceptable Use Agreement or any of the District's or a school's policies, regulations procedures or guidelines, access to the District's educational technology resources may be denied and other legal or disciplinary action may be taken.

(cf. 3513.3 - Tobacco-Free Schools)

~~6.~~ 6. Students shall not use the system to engage in commercial or other for-profit activities.

7. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.

8. Copyrighted material shall not be placed on the system without the author's permission and in accordance with copyright laws. Students may download copyrighted material for their own use only and with proper credit given, as with any other printed source of information.

(cf. 5131.9 Academic Honesty
cf. 6162.6 - Use of Copyrighted Materials)

~~7~~9. Students shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

(cf. 5131.5 - Vandalism, Theft and Graffiti)

~~8~~10. Students shall not read or use other users' electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to delete, copy, modify or forge other users' mail.

~~9~~11. Students shall report any security problem or misuse of the services to the teacher or principal.

The district reserves the right to monitor ~~any on-line communications~~ the use of the district's system for improper use without advance notice or consent. Electronic communications and downloaded material, including files deleted from a user's account, may be monitored or read by district officials to ensure proper use of the system.

(cf. 5145.12 - Search and Seizure)

Whenever a student is found to have violated Board policy, administrative regulation, or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

~~The principal or designee shall make all decisions regarding whether or not a student has violated Board policy or the district's Acceptable Use Agreement. The decision of the principal or designee shall be final.~~

~~Inappropriate use shall result in a cancellation of the student's user privileges, disciplinary action and/or legal action in accordance with law and Board policy.~~

(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))

7/14/04:4/14A

OAKLAND UNIFIED SCHOOL DISTRICT
Board Policy

BP 6163.4
Instruction

Student Use of Technology/ Internet Safety Policy

The Governing Board intends that technological resources used to access District equipment and networks whether provided by the district or ~~personal property~~the student be used in a responsible and proper manner in support of the instructional program and for the advancement of student learning.

The following policy and corresponding regulations and procedures are intended to implement the legal requirements of the district under The Children's Internet Protection Act, (CIPA) (Public Law 106-554). Such policy, regulations and procedures shall be applied to all students having computers or devices with Internet access. It is the policy of the Governing Board to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, social media, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors; and (d) comply with the Children's Internet Protection Act.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 4040 - Employee Use of Technology)
(cf. 6010 - Goals and Objectives)
(cf. 6162.7 - Use of Technology in Instruction)
(cf. 6163.1 - Library Media Centers)

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district computers and consequences for unauthorized use and/or unlawful activities.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process: Students with Disabilities)
(cf. 5145.12 - Search and Seizure)

Definitions

1. Access to the Internet - A computer shall be considered to have access to the Internet if such computer ~~is equipped with a modem or~~ is connected either wired or wirelessly to a computer network which has access to the Internet.

2. Minor shall mean an individual who has not attained the age of 19.

3. Obscene shall have the meaning given such term in section 1460 of title 18, United States Code.

4. Child pornography shall have the meaning given such term in section 2256 of title 18, United States Code.

5. Harmful to minors shall mean 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

6. Hacking shall mean attempting to gain unauthorized access to computer and network systems connected to the Internet.

7. Technology protection measure shall refer to the systems in place, managed by the district that blocks and/or filters Internet access.

On-Line Services/Internet Access

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors, and that the operation of such measures is enforced. (20 USC 7001, 47 USC 254) Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

The Board desires to protect students from access to harmful matter on the Internet or other on-line services and to prevent inappropriate network access. The Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to prevent inappropriate network access including hacking, unauthorized disclosure, use, and dissemination of personal identification information regarding minors, and other unlawful activities. He/she also shall establish regulations to address the safety and security of students when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communication.

Disclosure, use and dissemination of personal identification information regarding students is prohibited.

The Superintendent or designee shall oversee the education, supervision and monitoring of students' usage of the online computer network and access to the Internet in accordance with this

policy and applicable laws. The site principals or designated representatives shall provide age-appropriate training for students who use the District's Internet systems. The training provided shall be designed to promote the District's commitment to:

a. The standards and acceptable use of Internet services as set forth in this Policy;
b. Student safety with regard to: (1) safety on the Internet, (2) appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms; and (3) cyberbullying awareness and response, including that "bullying" constitutes any severe or pervasive physical or verbal act or conduct, including communications made in writing or by means of an electronic act that relates to school activity or attendance occurring under the jurisdiction of the school district's superintendent, including off-campus and/or electronic acts. (cf. Students Conduct 5131);
c. Prohibition of discrimination, harassment, intimidation, and bullying on the basis of actual or perceived protected characteristic, including without limitation, disability, gender, gender identity, gender expression, nationality, race or ethnicity, religion, sexual orientation or association with person or group with one or more of the actual or perceived characteristics; and
d. Compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies. Before using the district's on-line resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree to not hold the district responsible and shall agree to indemnify and hold harmless the district and all district personnel for the failure of any technology protection measures, violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

(cf. 6162.6 - Use of Copyrighted Materials)

Staff shall supervise students while they are using on-line services and may ask teacher aides and student aides to assist in this supervision.

In order to help ensure that the district adapts to changing technologies and circumstances, the Superintendent or designee shall regularly review this policy, the accompanying administrative regulation and other procedures. He/she shall also monitor the district's filtering software to help ensure its effectiveness.

Legal Reference:
EDUCATION CODE
48980 Required notification at beginning of term
51006 Computer education and resources
51007 Programs to strengthen technological skills

51870-51874 Education Technology
51870.5 Student Internet access
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 16
312.1-312.12 Children's online privacy protection
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
PUBLIC LAW 107-110
2401-2441 Enhancing Education Through Technology Act, No Child Left Behind Act, Title II, Part D
2441 Internet Safety

Management Resources:
CDE PUBLICATIONS
K-12 Network Technology Planning Guide: Building the Future, 1994
CDE PROGRAM ADVISORIES
1223.94 Acceptable Use of Electronic Information Resources
WEB SITES
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov
Commission on Online Child Protection: http://www.copacommission.org
CDE: http://www.cde.ca.gov
American Library Association: http://www.ala.org
CSBA: http://www.csba.org

7/14/04; 6/27/12A

OAKLAND UNIFIED SCHOOL DISTRICT
Board Policy

BP 6163.4
Instruction

Student Use of Technology/ Internet Safety Policy

The Governing Board intends that technological resources used to access District equipment and networks whether provided by the district or the student be used in a responsible and proper manner in support of the instructional program and for the advancement of student learning.

The following policy and corresponding regulations and procedures are intended to implement the legal requirements of the district under The Children's Internet Protection Act, (CIPA) (Public Law 106-554). Such policy, regulations and procedures shall be applied to all students having computers or devices with Internet access. It is the policy of the Governing Board to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, social media, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors; and (d) comply with the Children's Internet Protection Act.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 4040 - Employee Use of Technology)
(cf. 6010 - Goals and Objectives)
(cf. 6162.7 - Use of Technology in Instruction)
(cf. 6163.1 - Library Media Centers)

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district computers and consequences for unauthorized use and/or unlawful activities.

(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)
(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process: Students with Disabilities)
(cf. 5145.12 - Search and Seizure)

Definitions

1. Access to the Internet - A computer shall be considered to have access to the Internet if such computer is connected either wired or wirelessly to a computer network which has access to the Internet.

2. Minor shall mean an individual who has not attained the age of 19.

3. Obscene shall have the meaning given such term in section 1460 of title 18, United States Code.

4. Child pornography shall have the meaning given such term in section 2256 of title 18, United States Code.

5. Harmful to minors shall mean 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

6. Hacking shall mean attempting to gain unauthorized access to computer and network systems connected to the Internet.

7. Technology protection measure shall refer to the systems in place, managed by the district that blocks and/or filters Internet access.

On-Line Services/Internet Access

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors, and that the operation of such measures is enforced. (20 USC 7001, 47 USC 254) Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

The Board desires to protect students from access to harmful matter on the Internet or other on-line services and to prevent inappropriate network access. The Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to prevent inappropriate network access including hacking, unauthorized disclosure, use, and dissemination of personal identification information regarding minors, and other unlawful activities. He/she also shall establish regulations to address the safety and security of students when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communication.

Disclosure, use and dissemination of personal identification information regarding students is prohibited.

The Superintendent or designee shall oversee the education, supervision and monitoring of students' usage of the online computer network and access to the Internet in accordance with this

policy and applicable laws. The site principals or designated representatives shall provide age-appropriate training for students who use the District's Internet systems. The training provided shall be designed to promote the District's commitment to:

a. The standards and acceptable use of Internet services as set forth in this Policy;
b. Student safety with regard to: (1) safety on the Internet, (2) appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms; and (3) cyberbullying awareness and response, including that "bullying" constitutes any severe or pervasive physical or verbal act or conduct, including communications made in writing or by means of an electronic act that relates to school activity or attendance occurring under the jurisdiction of the school district's superintendent, including off-campus and/or electronic acts. (cf. Students Conduct 5131);
c. Prohibition of discrimination, harassment, intimidation, and bullying on the basis of actual or perceived protected characteristic, including without limitation, disability, gender, gender identity, gender expression, nationality, race or ethnicity, religion, sexual orientation or association with person or group with one or more of the actual or perceived characteristics; and
d. Compliance with the E-rate requirements of the Children's Internet Protection Act.

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies. Before using the district's on-line resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree to not hold the district responsible and shall agree to indemnify and hold harmless the district and all district personnel for the failure of any technology protection measures, violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

(cf. 6162.6 - Use of Copyrighted Materials)

Staff shall supervise students while they are using on-line services and may ask teacher aides and student aides to assist in this supervision.

In order to help ensure that the district adapts to changing technologies and circumstances, the Superintendent or designee shall regularly review this policy, the accompanying administrative regulation and other procedures. He/she shall also monitor the district's filtering software to help ensure its effectiveness.

Legal Reference:
EDUCATION CODE
48980 Required notification at beginning of term
51006 Computer education and resources
51007 Programs to strengthen technological skills

51870-51874 Education Technology
51870.5 Student Internet access
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 16
312.1-312.12 Children's online privacy protection
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
PUBLIC LAW 107-110
2401-2441 Enhancing Education Through Technology Act, No Child Left Behind Act, Title II, Part D
2441 Internet Safety

Management Resources:
CDE PUBLICATIONS
K-12 Network Technology Planning Guide: Building the Future, 1994
CDE PROGRAM ADVISORIES
1223.94 Acceptable Use of Electronic Information Resources
WEB SITES
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov
Commission on Online Child Protection: http://www.copacommission.org
CDE: http://www.cde.ca.gov
American Library Association: http://www.ala.org
CSBA: http://www.csba.org

7/14/04; 6/27/12A