Board Office Use: **Legislative File Info.**	
File ID Number	12-1779
Introduction Date	6-27-12
Enactment Number	12-1630
Enactment Date	6/27/12

OAKLAND UNIFIED SCHOOL DISTRICT

Community Schools, Thriving Students

Memo

To Board of Education

From Maria Santos, Deputy Superintendent
Gee Kin Chou, Executive Officer Technology Services

Board Meeting Date June 27, 2012

Subject Modification to Board Policy 6163.4 Student Use of Technology

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

Background
A one paragraph explanation of the Board Policy is needed.

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
One paragraph summary of the Board Policy.

The modifications to the Board Policy incorporate changes that are required by recent state and federal legislation, including the Children's Internet Protection Act, and state legislation relating to bullying. The modifications to the policy are required to be implemented by the District for participation in the E-Rate program. The modifications provide for age-appropriate education of minors about appropriate online behavior, including education about appropriate interaction with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. The modifications also provide an updated definition of bullying in accordance with changes in state law and expressly specify that bullying can include electronic acts. The modifications to the policy also incorporate updates in anti-discrimination laws which will be included in the training to students.

Recommendation Approval of the modifications to Board Policy 6163.4 Student Use of Technology

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)

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 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 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, 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 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.

Formatted: Bullets and Numbering

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.

~~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)~~

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

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 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 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. 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 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