San Diego Unified
SCHOOL DISTRICT

ADMINISTRATIVE PROCEDURE

EFFECTIVE: 4-18-95
REVISED: **11-15-13**

CATEGORY: Instruction, Instructional Services

SUBJECT: **Student Use of District and School Data Communications Networks and Internet Safety Policy**

A. PURPOSE AND SCOPE

1. To outline rules governing students' use of district and school data communications networks, the intranet, and internet safety and to provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

2. **Related Procedures:**

B. LEGAL AND POLICY BASIS

1. **Reference:** Board Policies A-3550 (approved 4-12-11) and G-7500; Education Code sections 51870-51874; California Penal Code sections 313 and 502; Children's Internet Protection Act H.R. 4577; United States Code Title 18 sections 1460, 2246, and 2256; 47 United States Code section 254(h); Public Law 106-554

2. **Access to Harmful Matter.** Education Code requires school districts that provide students with access to the internet or to an online service to adopt a policy regarding access to sites that contain or make reference to harmful matter as defined in Penal Code section 313 subdivision (a). "Harmful matter" means that, taken as a whole, the predominant appeal of which to the average person, applying contemporary standards, is to prurient interest (i.e., a shameful or morbid interest in nudity, sex, or excretion); matter which taken as a whole goes substantially beyond customary limits of candor in description or representation of such matters; and matter which taken as a whole is utterly without redeeming social importance for minors.

3. **Children's Internet Protection Act (CIPA) Compliance.** It is the policy of the district 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 or other unlawful online activity;

   c. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

   d. Comply with the Children's Internet Protection Act (CIPA), Public Law 106-554 and 47 United States Code section 254(h).

C. GENERAL

1. **Originating Office.** Questions concerning this procedure should be directed to Integrated Technology Support Services (ITSS) or the Educational Technology Department. Suggestions concerning this procedure should be directed to ITSS.

2. **Definitions.**

   a. **Network:** Two or more computer systems linked to allow communication. The district's network connects schools and support offices to provide data communications, such as e-mail, file sharing, and internet access.

   b. **Internet:** A global computer network.

   c. **World Wide Web (www):** A global, hypertext-based information system accessible through the internet via HTTP protocol.

   d. **Universal Resource Locator (URL):** The address of a source of information on the internet.

   e. **E-Mail:** Electronic mail messaging over communications network.

   f. **File server:** A shared computer providing data storage and services to users.

   g. **District data:** Information maintained and processed in the conduct of district business as required by state or federal mandate and/or district procedure. Confidentiality restrictions may apply to information maintained as district data records and to all copies of those records.

   h. **System administrator:** Person(s) responsible for providing and/or managing network services (e.g., file servers, electronic mail, and internet services).

   i. **Security administrator:** Person(s) responsible for providing network security.

   j. **Network Use Guidelines:** District guidelines for students and parents/guardians regarding acceptable use of the internet and district networks (Attachment 1)

   k. **Student Network Responsibility Contract:** A contract between a student and parent/guardian and a school regarding acceptable use of the internet and district networks. The student and his/her parent guardian must sign this contract upon enrolling in a district school. A contract must be signed at each new district school in which the student is enrolled (Attachment 2).

   l. **Technology protection measure:** A specific technology that blocks or filters internet access to visual depictions that are:

      (1) Obscene, as the term is defined in United Sates Code Title 18 section 1460;

      (2) Child pornography, as that term is defined in United States Code Title 18 section 2256; or

      (3) Harmful to minors.

m. **Harmful to minors:** Any picture, image, graphic image file, or other visual depiction that:

(1) Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

(2) 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

(3) Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

n. **Sexual act, sexual contact:** As defined in United States Code Title 18 section 2246.

o. **Minor:** For the purposes of this procedure, any individual who has not attained the age of 17.

p. **Child pornography:** As defined in United States Code Title 18 section 2256.

q. **Computer:** Any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with an electronic data processor.

r. **Obscene:** As defined in United States Code Title 18 section 1460.

3. **Acceptable Use.** The use of district network services is a privilege and is to be limited to district business as authorized by Board policy. School-level practice should support and complement district policy and procedure and should be tied to specific curriculum goals and objectives. Use of the district's network services by district employees should support district policy and procedure in the performance of their assigned duties.

4. **Prohibited Use.**

a. Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to distribution of:

(1) Any information that violates or infringes upon the rights of any other person.

(2) Any defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

(3) Advertisements, solicitations, commercial ventures, or political lobbying.

(4) Any information that encourages the use of controlled substances or the use of the system for the purpose of inciting crime.

(5) Any material that violates copyright laws (Administrative Procedure 7038).

b. Any vandalism, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited (California Penal Code section 502).

c. Inappropriate use may result in cancellation of network privileges. The site system administrator(s) or district security administrator may close an account at any time deemed necessary. Depending upon the seriousness of the offense, any combination of the following will be enforced: Penal Code, Education Code, district procedures, or school site discipline/network use policy.

d. The district reserves the right to monitor internet/intranet, e-mail, and networked application usage. No student or employee should have any expectation of privacy as to his/her usage. The district reserves the right to inspect any and all files on district computers or district servers connected to district networks and to take custody and possession of those files and computers.

5. **Etiquette.** The use of the district's data communications networks requires that users abide by accepted rules of network etiquette. These include, but are not limited to:

a. **Be polite.** Do not send abusive, inflammatory, or obscene messages to others. Use language that is appropriate for an educational setting.

b. **Respect privacy.** Do not reveal personal information about students or staff.

c. **Be considerate.** Do not use the network in a way that would disrupt the use of the network by other users.

6. **Electronic Mail.** Users of electronic mail systems should not consider electronic communication to be either private or secure; such communications are subject to review by authorized district personnel and may be subject to review by the public under the Public Records Act. Messages relating to or in support of illegal activities must be reported to appropriate authorities. Other conditions for use include, but are not limited to:

a. Individuals are to identify themselves accurately and honestly in e-mail communications. E-mail account names and/or addresses may not be altered to impersonate another individual or to create a false identity.

b. The district retains the copyright to any material deemed to be district data. Use of district data sent as e-mail messages or as enclosures will be in accordance with copyright law and district standards.

7. **Responsibilities.**

a. **Reasonable precautions by district staff.** The district maintains reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. Staff will choose resources on the internet that are appropriate for classroom instruction and/or research for the needs, maturity, and ability of their students. However, parents/guardians, students, and staff should understand that on a public network, it is not possible to control *all* material and accept

responsibility for complying with district procedures and with standards of acceptable use.

b. **Guidelines for parents/guardians and students.** A copy of "Network Use Guidelines" (Attachment 1) must be provided to parents/guardians of students to whom the guidelines apply. Students and parents/guardians accept responsibility for abiding by the "Network Use Guidelines" and understand that violation can result in loss of access privileges and disciplinary action.

c. **Publications of student information.** Before publishing a student's picture, name, or work for display on an internet page, the school must have on file a parent release form authorizing publication (Attachment 3).

d. **Education, Supervision and Monitoring.** It is the responsibility of all district staff members to educate, supervise, and monitor appropriate usage of the online computer network and access to the internet in accordance with this procedure and CIPA, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of ITSS or designated representatives.

ITSS will assist schools by providing training materials and online resources for age-appropriate training of students who use the district's internet facilities. Each school principal is responsible for ensuring that each student receives this training before accessing the district's internet facilities. The training provided will be designed to promote the district's commitments to:

(1) The standards and acceptable use of internet services as set forth in this procedure and internet safety policy;

(2) Student safety with regard to safety on the internet; appropriate behavior while online, on social networking websites, and in chat rooms; and cyberbullying awareness and response.

(3) Compliance with CIPA E-rate requirements.

Following participation in this training, each student will acknowledge that he/she has received the training, understands it, and will adhere to the provisions of the district's acceptable use policies.

8. **Technology Protection Measures.** To the extent practical, technology protection measures (or "internet filters") shall be used to block or filter inappropriate information via internet access or forms of electronic communications. Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. 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.

To the extent practical, steps shall be taken to promote the safety and security of users of the district's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes:

a. Unauthorized access, including "hacking," and other unlawful activities; and

b. Unauthorized disclosure, use and dissemination of personal identification information regarding minors.

9. **Security.** Security on any computer system is a high priority, especially in a system with many users. If any user identifies a security problem with district systems, he/she must notify the ITSS security administrator either in person or in writing, or via the network. Users should not demonstrate the problem to other users. Any user identified as a security risk or having a history of problems with other computer systems may be denied network access. Violations include, but are not limited to:

a. Illicitly gaining entry, or "hacking" into a computer system or obtaining account passwords.

b. Intentionally creating or distributing a computer virus.

c. Using district systems or equipment to knowingly disable or overload any computer system or network or to circumvent the security of a computer system.

d. Knowingly bypassing a district "firewall" used for blocking inappropriate internet sites and for security screening.

D. IMPLEMENTATION

1. Each student shall receive internet safety training, in accordance with section C(7)(d) of this procedure and must acknowledge that he/she received the training, understands it, and will adhere to this procedure and the district's "Network Use Guidelines" (Attachment 1).

2. Before each student is provided access to the internet or any district network, schools shall provide a copy of "Network Use Guidelines" (Attachment 1) to parents/guardians.

3. Students shall be provided access to the internet or to the district network only after receipt of the training in Section C(7)(d) of this procedure and after submission of his/her signed "Student Network Responsibility Contract" (Attachment 2) to the school, which school shall keep on file.

4. School shall obtain or have on file a parent/guardian release form (Attachment 3) authorizing publication of a student's picture, name, or work on the internet.

E. FORMS AND AUXILIARY REFERENCES

1. Network Use Guidelines, Attachment 1

2. Student Network Responsibility Contract, Attachment 2

3. Parent/Guardian Release Form, Attachment 3

F. REPORTS AND RECORDS

1. Attachments 2 and 3, with parent/guardian/student signature, are to be retained at the school site.

G. APPROVED BY

General Counsel, Legal Services
As to form and legality

H. ISSUED BY

Chief of Staff