DEL MAR UNION SCHOOL DISTRICT
INSTRUCTION

BOARD POLICY 6163.4 (was BP 6017): STUDENT USE OF TECHNOLOGY

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

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district computers, user obligations and responsibilities, as well as consequences for unauthorized use and/or unlawful activities in accordance with district regulations and the Acceptable Use Agreement.

Before a student is authorized to use the district's technological resources, each student and his/her parent/guardian shall sign and return the Student 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 or any district staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' mistakes or negligence. They shall also agree to indemnify and hold harmless the district and all district personnel for any damages or costs incurred.

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update this policy, the accompanying administrative regulation, and other relevant procedures to enhance the safety and security of students using the district's technological resources and to help ensure that the district adapts to changing technologies and circumstances.

Use of District Owned Devices for Online 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 6777, 47 USC 254.)

The Board desires to protect students from access to inappropriate matter on the Internet or other online services. The Superintendent or designee shall establish regulations to address the safety and security of students and student information when using electronic mail, chat rooms and other forms of direct electronic communication.

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016

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)

The district's Acceptable Use Agreement shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

1. Accessing, posting, submitting, publishing, or displaying 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, sex, gender, sexual orientation, age, disability, religion, or political beliefs

2. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking"

3. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting one's own personal identification information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016

Legal Reference:

EDUCATION CODE
48900 Suspension and Expulsion
49073.6 Student records; social media
51006 Computer education and resources
51007 Programs to strengthen technological skills
51870-51874 Education Technology
60044 Prohibited instructional materials
PENAL CODE
313 Harmful matter
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
653.2 Electronic communication devices, threats to safety
1546 Electronic Communications Privacy Act
UNITED STATES CODE, TITLE 15
6501-6506 Children's Online Privacy Protection Act
UNITED STATES CODE, TITLE 20
6751-6777 Enhancing Education Through Technology Act, No Child Left Behind Act, Title II, Part D
6777 Internet safety
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

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
CDE: http://www.cde.ca.gov
American Library Association: http://www.ala.org
CSBA: http://www.csba.org

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016

DEL MAR UNION SCHOOL DISTRICT
INSTRUCTION

ADMINISTRATIVE REGULATION TO BOARD POLICY 6163.4 (was BP 6017): STUDENT USE OF TECHNOLOGY

The principal or designee shall oversee the maintenance of each school's technological resources and may establish guidelines and limits on their use. He/she shall ensure that all students using these resources receive training in their proper and appropriate use.

The principal or designee shall 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.

Online/Internet Services: User Obligations and Responsibilities

Students are authorized to access the Internet or online 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 online services account is issued, is responsible for its proper use at all times. Students shall keep personal account numbers, home addresses and telephone numbers private. They shall use the system only under their own account number.

2. Students shall use the district's system 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.

   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.)

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016

4. Unless otherwise instructed by school personnel, 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.

6. Copyrighted material shall not be placed on the system without the author's permission. Students shall not violate copyright laws or plagiarize documents. Any materials utilized for research projects should be given proper credit as with any other hard copy sources of information.

7. 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."

8. Students shall not read 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. Students shall report any security problem or misuse of the services to the teacher or principal.

Federal law requires the district to implement technology protection measures, which include filtering and monitoring of use of district technology. As such, there should be no expectation of privacy when using district technology and/or the district network. The district reserves the right to monitor the system for improper use. Electronic communications and downloaded material, including files deleted from a user's account, email and all materials found or created on district time and equipment, may be accessible to the district to ensure proper use of the system. 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.

00118-00005/3206351.1

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016

Adopted 01/13/1999 (was BP 6017)
Revised: 01/23/2008
Revised: 12/14/2011
Revised: 5/25/2016