The County Superintendent of Schools intends that the Internet and other technological resources be used to support the instructional program and further student learning. The County Superintendent of Schools recognizes that technology provides ways to access the most current and extensive sources of information. Technology also enables students to practice skills and to develop reasoning and problem-solving abilities. Every effort will be made to provide equal access to technology throughout the schools, programs, and facilities operated by the County Superintendent of Schools.

This administrative regulation presents obligations and responsibilities of students in the use of San Diego County Office of Education (SDCOE) technological resources. Technological resources refer to all equipment; software; electronic networks, both wired and wireless; websites and content; and licenses that are owned, leased, or operated by the San Diego County Office of Education. Exhibit 1 presents definitions of SDCOE technological resources.

This regulation implements the Internet safety requirements of the Children's Internet Protection Act (CIPA) and the Protecting Children in the 21st Century Act to safeguard minors and ensure eligibility for Universal Service (E-rate) discounts on Internet access, telecommunications services, and other eligible products and services. The Internet safety policy of the San Diego County Office of Education includes educating students in schools and programs operated by the County Superintendent of Schools regarding appropriate online behavior and cyberbullying and response, monitoring of online activities of minors, and the operation of a technology protection measure that filters and blocks access to visual depictions that are obscene, child pornography, or harmful to minors.

Supervision, Monitoring, and Filtering

The County Board of Education and the County Superintendent of Schools do not control the content of information or resources accessible on the Internet. Students, parents, and teachers or other supervising adults should be aware that some of the materials available online may be controversial and inappropriate for access by

students. The County Superintendent encourages student use of technological resources in a responsible, safe, and age-appropriate manner.

Under reasonable supervision of instructional staff and other authorized adults, students may use the Internet and online resources provided for educational purposes in the schools, programs, and facilities operated by the County Superintendent of Schools.

Students should be aware that computer files and communications over electronic networks, including e-mail and voice mail, are not private. The County Superintendent reserves the right to monitor, examine, and reasonably restrict system activities to ensure appropriate use of technological resources by students at any time without advance notice or consent. Electronic communications, Internet use, and downloaded material, including files deleted from a student's account under specific conditions, may be monitored or read by teachers and other employees.

In compliance with Federal Communications Commission rules for CIPA, a technology protection measure shall continuously filter Internet access in the schools and programs operated by the County Superintendent of Schools and at SDCOE Regional Education Center facilities. Students are prohibited from using computers with Internet access where the technology protection measure is not enabled.

Student Use in Schools and Programs Operated by the County Superintendent of Schools

The assistant superintendent, Student Services and Programs, or designee shall enforce a policy of Internet safety in the schools and programs operated by the County Superintendent of Schools. In compliance with Federal Communications Commission rules for the Protecting Children in the 21st Century Act, instruction shall be provided to students regarding appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response.

A *Student Services and Programs Acceptable Use Agreement* that specifies student obligations and responsibilities in the use of SDCOE technological resources and the

consequences of misuse and unlawful activities as presented in this administrative regulation shall be maintained and enforced.

Upon the initial enrollment of a student and at the beginning of each school year thereafter, a school or program administrator designated by the assistant superintendent, Student Services and Programs, shall notify each student enrolled in the school(s) or program under his/her direction and the student's parent or guardian regarding acceptable use of SDCOE technological resources, including access to the Internet by students. This notification shall include a copy of the *Student Services and Programs Acceptable Use Agreement* enforced by the San Diego County Office of Education. Before a student may use SDCOE technological resources, the student's parent or guardian shall be required to sign and submit a copy of the *Student Services and Programs Acceptable Use Agreement* to the designated school or program administrator.

The designated school or program administrator shall make all decisions regarding whether a student has violated conditions of the *Student Services and Programs Acceptable Use Agreement*, SDCOE administrative regulation, or Board policy. A student's access to SDCOE technological resources may be suspended, terminated, denied, or revoked at any time, and disciplinary and/or legal action may be pursued. In the event of a dispute regarding the decision of the school or program administrator, the matter may be appealed to the assistant superintendent, Student Services and Programs.

The decision of the assistant superintendent, Student Services and Programs, shall be final.

Student Use at SDCOE Regional Education Centers and Other SDCOE Facilities

Students enrolled in schools and programs that are not operated by the County Superintendent of Schools may be provided access to SDCOE technological resources at an SDCOE regional education center or other SDCOE facility. The assistant superintendent, Integrated Technology Services, or designee(s) shall enforce a policy of Internet safety in the use of SDCOE technological resources by those students.

Prior to student use of technological resources at SDCOE facilities, the designated supervising adult shall be required to submit a signed Information Technology Services *Acceptable Use Agreement for Student Use of SDCOE Technological Resources.* The agreement shall require the supervising adult to inform students of their obligations and responsibilities in the use of SDCOE technological resources as presented in this administrative regulation and to oversee their compliance.

In the event that a student violates his/her obligations and/or responsibilities, the assistant superintendent, Integrated Technology Services, or designee may suspend, terminate, or deny the student access to SDCOE technological resources.

Student Obligations and Responsibilities

Students are authorized to use technological resources of the San Diego County Office of Education, as defined in Exhibit 1 of this administrative regulation, in accordance with the obligations and responsibilities specified below.

1. Students shall not disclose, use, distribute, publish, e-mail, hyperlink, or make available for downloading personal identifying information about themselves or anyone else when using the Internet, e-mail, chat rooms, or other forms of direct electronic communication unless specifically authorized to do so. Personal identifying information includes, but is not limited to, digital images, full names, personal account access information, home addresses, phone numbers, Social Security numbers, and any other individually identifiable information.

2. Students shall not use technological resources for commercial or other for-profit activities, political or religious purposes, or personal use unrelated to an educational purpose.

3. Students shall not use technological resources to encourage the use of drugs, alcohol, or tobacco, to promote or participate in unethical practices such as cheating and plagiarism, or to conduct any activity prohibited by law, Board policy, or administrative regulation.

4. Students are prohibited from accessing, downloading, posting, transmitting, publishing, or displaying harmful matter or any content that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of any member of a group protected by state or federal law.

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

5. Students shall not use technological resources to engage in cyberbullying.

   Cyberbullying means any severe or pervasive act or conduct inflicted by means of an electronic act, including, but not limited to, sexual harassment; hate violence; or harassment, threats, or intimidation, as those terms are defined in Education Code sections 48900.2, 48900.3, and 48900.4, respectively. Cyberbullying occurs when such conduct is directed toward one or more students and has or can be reasonably predicted to have the effect of one or more of the following:

   A. Placing a reasonable student in fear of harm to the student's person or property.

   B. Causing a reasonable student to experience a substantially detrimental effect on his/her physical or mental health.

   C. Causing a reasonable student to experience substantial interference with his/her academic performance.

D. Causing a reasonable student to experience substantial interference with his/her ability to participate in or benefit from the services, activities, or privileges provided by a school.

Cyberbullying includes using another person's electronic account for any of the purposes listed above.

Electronic act means the transmission of a communication, including but not limited to, a message, text, sound, image, or post on a social networking website, by means of an electronic device, including, but not limited to, a telephone, wireless telephone or other wireless communication device, computer, or pager.

Reasonable student means a student, including, but not limited to an exceptional needs student, who exercises average care, skill, and judgment in conduct for a person of his/her age, or for a person of his/her age with his/her exceptional needs.

Students are further prohibited from using technological resources to engage in harassment, intimidation, or threats of any kind to any individual, including students, instructional staff, and administrators.

6. Students shall not connect to social networking websites unless specific authorization has been granted for purposes consistent with the educational program. Participation in social networking websites must be in strict compliance with the Student Obligations and Responsibilities presented in this administrative regulation.

7. Students shall not download, post, transmit, or publish copyrighted material, including multimedia and software, except as permitted by copyright law or with appropriate permission or license.

8. Students shall not knowingly access and without permission read, delete, copy, or modify other users' e-mail messages or files, interfere with other users' ability to send or receive e-mail messages, or forge or fraudulently use other users' e-mail or files.

9. Students shall not commit acts of vandalism, including but not limited to, hacking, intentionally uploading, downloading, transferring, or creating computer viruses and/or any malicious or unauthorized use of SDCOE technological resources. Also included are any actions that attempt to harm or destroy equipment or materials or manipulate the data, in any form, of any other user. Public offenses related to computer crime are further defined in Penal Code section 502.

10. Students shall not purposefully disable or circumvent any technology protection measure installed on SDCOE technological resources.

Annual Review

The assistant superintendent, Student Services and Programs, and the assistant superintendent, Integrated Technology Services, or designees, shall annually review and, if indicated update, this administrative regulation, acceptable use agreements, and related procedures to adapt to changing technologies and circumstances and ensure the continuing safety and security of students using SDCOE technological resources.

Board Policy: 2303, 3600, 5145
Administrative Regulation: 2300, 3600

Derivation: Adopted 3/22/00. Public hearing 2/4/03. Amended 2/4/03, 6/28/12.

Legal References: Education Code
200 et seq., 260, 32261, 48900 et seq., 48980, 51006 - 51007, 51870 - 51874
Government Code
11135
Penal Code
311, 313, 422.55 - 422.6, 502, 632, 653.2
United States Code, Title 15
Children's Online Privacy Protection Act (COPPA), sections 6501 - 6502
United States Code, Title 17
101 - 122
United States Code, Title 18
2256
United States Code, Title 20
6751 - 6777

United States Code, Title 47
254(h), 254(l)
Children's Internet Protection Act (CIPA), section 1721 et seq.
Protecting Children in the 21st Century Act, section 215
Code of Federal Regulations, Title 16
312.5
Code of Federal Regulations, Title 34
100.3
Code of Federal Regulations, Title 47
54.500 - 54.520
FCC 11-125 Report and Order, Adopted August 10, 2011
FCC 01-120 Report and Order, Adopted March 30, 2001
Public Law 107-110
No Child Left Behind Act of 2001, sections 2401-2441
Public Law 110-385
Broadband Data Services Improvement Act, sections 211, 215

Management Resources:

California Department of Education: Federal Telecommunications Discounts for Schools and Libraries – http://www.cde.ca.gov/ls.et.ft/eratemain.asp
Federal Communications Commission: www.fcc.gov
Integrated Technology Services Acceptable Use Agreement: www.sdcoe.net/pdf/ITS-AUA.pdf
Student Services and Programs Acceptable Use Agreement
Student Services and Programs Acceptable Use Agreement: https://www.sdcoe.net/fs/resource-manager/view/e0f74b76-249e-4fc9-8be6-4e83cb2b27b6
USAC Schools and Libraries Division (SLD): www.sl.universalservice.org/

EXHIBIT 1 – AR 6163
Page 1 of 1
Adopted: 6/28/12

DEFINITIONS OF TERMS

Technological resources of the San Diego County Office of Education (SDCOE) refer to equipment, software, electronic networks, web sites and content, and licenses that are owned, leased, or operated by SDCOE including, but not limited to the following:

1. Equipment: All desktop, laptop, tablet, and portable computers; telephones and cellular phones; personal digital assistants (PDAs); and peripheral devices, including printers, scanners, and external or removable storage devices

2. Software: Operating systems; off-the-shelf applications; operating system and browser extensions; and CD-ROMs, DVDs and electronic downloads containing applications and installers

3. Software as a Service (SaaS): Application software that is Internet-based and is not installed on local workstations. Examples are Zoho, Google Apps, and Microsoft Office Live.

4. Electronic Networks: Equipment, cabling, software, and data circuitry that provide wired and wireless connections among SDCOE facilities, commercial Internet access (including services granted by the K12 High Speed Network), and interconnection of SDCOE servers and workstations

5. Websites and content: All web sites hosted on equipment owned or leased by SDCOE and all websites bearing the San Diego County Board of Education copyright, including the underlying text, pictures, data, and presentation of information that comprises static and dynamic web page content

6. Licenses: All documentation, activation keys and codes, and rights to use and/or redistribute that are purchased by or granted to SDCOE for the purpose of using copyrighted software