Instruction

STUDENT USE OF TECHNOLOGY AND INTERNET SAFETY

The Board of Trustees intends that technological resources provided by the District be used in a safe, 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, and consequences for unauthorized use and/or unlawful activities in accordance with District regulations and the District's Acceptable Use Agreement.

The Superintendent or designee shall provide age-appropriate instruction regarding the District's acceptable use agreement, including instruction on the safe use of social networking sites and other Internet services including, but not limited to, the dangers of posting personal information online, misrepresentation by online predators, and how to report inappropriate or offensive content or threats.

The Superintendent or designee, with input from students and appropriate staff, shall regularly review this policy, the accompanying administrative regulation, and other relevant procedures to help ensure that the District adapts to changing technologies and circumstances.

Use of District Computers for Online Services/Internet Access

The Superintendent or designee shall ensure that all District computers with Internet access have a technology protection measure designed to block or filter Internet access to visual, verbal and printed depictions that are obscene, child pornography, subversive or harmful to minors, and that the operation of such measures is enforced.

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access, within reason, to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in this supervision.

The Superintendent or designee also shall establish regulations to address the safety and security of students and student information when using email, chat rooms, and other forms of direct electronic communication.

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 personal 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.

STUDENT USE OF TECHNOLOGY AND INTERNET SAFETY (continued)

Student use of District technology to access unauthorized sites, including unauthorized social networking sites, is prohibited. To the extent possible, the Superintendent or designee shall block access to such sites on District computers with Internet access.

Before using the District's technological resources, each student and his/her parent/guardian shall sign agreeing to the Student Internet/Software 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 District personnel for any damages or costs incurred.

Use of Student Personal Technology Devices for Internet Access

The Superintendent or designee shall make available to all students the opportunity to connect an approved personal technological device to the District provided guest wireless network for academic purposes. Students using their own device to connect to the guest wireless network must do so with their District issued individual account. If applicable, the personal device must have current anti-virus software installed before accessing the network. The device may be used in the classroom or learning space for academic purposes only. The individual school site may provide direction on expectations of utilization and device specifications, with guidance from the technology department and legal.

The Superintendent or designee shall establish guidelines for schools to implement "Bring Your Own Device" programs with clear procedures on ensuring equity of access and compliancy with Education Code 49011, prohibiting required student fees to participate in an educational activity.

The use of personal mobile devices, such as laptops, Smartphones, tablets, etc., by students on campus is subject to all applicable District policies and regulations concerning technology use, as well as the following rules and understandings:

- Permission to have a mobile device at school is contingent upon parent/guardian understanding this agreement except as required by Education Code section 48901.5(b)
- All costs for data plans and fees associated with mobile devices are the responsibility of the student. The District does not require the use of personal mobile devices in any instructional setting but may allow their use to enhance learning.
- Schools supporting subject or grade level programs where students participate in a Bring Your Own Device program will provide equity devices, equivalent to the current District standard, to ensure everyone has the opportunity to participate.
- Mobile devices with Internet access capabilities which are being harnessed for classroom learning purposes are required to use the District filtered guest network.
- Students are required to use their District issued individual account to access the guest wireless network at all times.
- Use during class time must be authorized by the teacher.

STUDENT USE OF TECHNOLOGY AND INTERNET SAFETY (continued)

- Students are directed not to photograph, video tape, or record any individuals without the written permission of the teacher or administrator and the students being photographed. Recordings made in a classroom require the advance written permission of the teacher or school principal.
- Students may not take, possess or share obscene photographs or videos.
- Students may not photograph, videotape or otherwise record instructional materials and assessments.
- The District assumes no responsibility for the loss, destruction or theft of any personal devices including, but not limited to, cellular phones, computers, or personal electronic devices. Devices should not be left unattended. School officials and District office staff are not required to investigate lost or stolen personal electronic equipment.
- The District is not responsible for online material accessed off campus on a non-District network.
- Students should not expect privacy in the contents of their personal files on the District network, District approved cloud storage systems, and records of their online activity. The District's monitoring of Internet usage can reveal all activities students engage in using the District network. Parents have the right to request to see the contents of their student's computer files at any time
- Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist with supervision. Parent/Guardian is exclusively responsible for monitoring his or her child(s) use of the Internet when off campus and when accessing District approved online educational systems from home or a non-school location. The District does not employ its filtering systems to screen home access to the District's online educational systems.
- Cyberbullying is prohibited by state law and District policy. Bullying or harassment that is done on or off campus with a computer or any type of communications device may result in discipline at school up to and including expulsion, legal action, or prosecution by the appropriate law enforcement authorities.

It will be each student's responsibility to follow the rules for appropriate and responsible use as detailed in the Student Internet/Software Acceptable Use Agreement. Access to the guest network is a privilege and administrators and staff may review files and messages to maintain system integrity and ensure that users are acting responsibly. The District is not responsible for theft, loss, or damage to personal technology devices that are brought to school from home by students.

STUDENT USE OF TECHNOLOGY AND INTERNET SAFETY (continued)

Legal References:

EDUCATION CODE
51006 Computer education and resources
51007 Programs to strengthen technological skills
51870- 51874 Education Technology Act especially:
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
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, Title II, Part D, especially:
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:
CSBA PUBLICATIONS
Cyberbullying: Policy Considerations for Boards, Governance and Policy Services Policy Brief, July 2007
FEDERAL TRADE COMMISSION PUBLICATIONS
How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
CDE PUBLICATIONS
K-12 Network Technology Planning Guide: Building the Future, 1995
CDE PROGRAM ADVISORIES
1223.94 Acceptable use of Electronic Information Resources
MY SPACE.COM PUBLICATIONS
The Official School Administrator's Guide to Understanding MySpace and Resolving Social Networking Issues
WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Coalition for Children's Internet Safety: http://wwwcybersafety.ca.gov
CDE: http://www.cde.ca.gov
Center for Safe and Responsible Internet Use: http://csriu.org and http://cyberbully,org
Federal Communications Commission: http//www.fcc.gov
U.S. Department of Education: http://www.ed.gov
Web Wise Kids: http://www.webwisekids.org

Policy
adopted: 6/14/99
revised: 10/1/01
revised: 1/14/08
revised: 2/11/08
revised: 12/4/09
revised: 1/12/10
revised: 6/10/15

CAPISTRANO UNIFIED SCHOOL DISTRICT
San Juan Capistrano, California