San Diego Cooperative Charter School Electronic Acceptable Use Policy

Statement of Purpose

San Diego Charter School (SDCCS) is pleased to offer our students theaccess to classroom computers (Chromebooks and iPads), the Internet, and other electronic networks. The advantages afforded by the rich, digital resources available today through the Internet outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved. Internet safety is an important concern.

Chromebooks, iPads and other devices are used as tools for research and education and, like any other school property, must be used for the educational purposes for which they are intended. The use of a Chromebook, iPad or other devices is a privilege, not a right, and may be revoked at any time for inappropriate conduct.

Policy Coverage

The policies, procedures, and information within this document apply to all technology used at SDCCS by students, staff, or guests (herein, all users referred to as “students”) including any other device or technology considered by the Administration to fall under this policy. Teachers may set additional requirements for Chromebook/iPad use in their classroom.

Children’s Internet Protection Act

It is the policy of SDCCS to (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of communications; (b) prevent unauthorized access and 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 [Pub. L No. 106-554 and 47 USC 254(h)].

COPPA - Children’s Online Privacy Protection Act

COPPA (Children’s Online Privacy Protection Act) causes any website that collects information such as name and email address (the information needed to create a unique account) to prohibit use by children under 13 without parental consent. Because of these guidelines, parents must give authorization for students to create online accounts or have teacher created online accounts, which are carefully selected for age and subject appropriate classroom use. Students will be supervised during in class use of all Internet tools.

Internet Safety

1. ***Parents and Users***. Despite the best efforts of supervision and Internet filtering, all users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and Internet and avoid these sites.
2. ***Personal Safety***. In using the network and Internet, users should not reveal personal information such as names, home address, telephone number, school name, location, etc. Users should never arrange a face- to-face meeting with someone “met” on the Internet without a parent’s permission.
3. ***Confidentiality of Student Information***. Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.
4. ***Active Restriction Measures***. SDCCS uses filtering software and other technologies to prevent students from accessing websites that are obscene, pornographic, harmful to minors, anti- social, or promote illegal activity. The use of anonymous proxies to bypass content filters is strictly prohibited and will be considered a violation of the acceptable use policy. The school also monitors the online activities of students, through direct observation and/or technological means.

School Responsibilities

* 1. Provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the school curriculum.
  2. Use networked resources in support of educational goals.
  3. Treat student infractions of the Computer and Internet Use Policy according to the school discipline policy.
  4. Provide alternate activities for students who do not have permission to use the Internet.

Student Use of Internet Tools

The use of blogs, podcasts, or other Internet tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of email, blogs, podcasts, or other Internet tools. This includes but is not limited to profanity, racist, sexist, bullying, or discriminatory remarks. Students contributing to the class blogs, podcasts or other web tools are expected to act safely by keeping ALL personal information out of their content. A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers).

Students who do not abide by these terms and conditions may lose their Internet access privileges as specified in the School Discipline Policy.

Education, Supervision, and Monitoring

It shall be the responsibility of all members of the SDCCS staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children’s Internet Protection Act, the Neighborhood Children’s Internet Protection Act, and the Protecting Children in the 21st Century Act.

Education for minors shall include appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms; and cyber bullying awareness and response.

Responsibility for Electronic Data

The students are solely responsible for any data, apps or extensions on their Chromebooks that are not installed by a member of the SDCCS technology staff. Students are responsible for backing up their data to protect from loss. Users of SDCCS Technology have no rights, ownership, or expectations of privacy to any data that is, or was, stored on the Chromebook, school network, or any school-issued applications and are given no guarantees that data will be retained or destroyed.

Access to Inappropriate Material

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet access to inappropriate information. 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 or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the SDCCS online computer network when using electronic mail and other forms of direct electronic communications. Specifically, as required by CIPA, prevention of inappropriate network usage includes (a) unauthorized access, including so-called ‘hacking’, and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Unacceptable Usage of Computers and Networks

The user is responsible for all his/her actions and activities involving the network. Examples of prohibited conduct include but are not limited to the following

1. Accessing materials/communications, or sending, creating, or posting materials that are
2. Damaging to another person’s reputation
3. Abusive
4. Obscene
5. Threatening or demeaning to a person’s gender or race
6. Sexually oriented
7. Contrary to the school’s policy on harassment
8. Illegal
9. Harassing / Cyberbullying
10. Gaining unauthorized access to wired or wireless network resources.
11. Using the school’s computers or network for illegal activity such as copying software or other violation of copyright laws.
12. Using the school’s network for private financial or commercial gain.
13. Loading or using games, public domain, shareware, or any other unauthorized programs on any of the school’s computers or computer systems.
14. Purposely infecting any school computer or network with a virus or program designed to damage, alter, or destroy data.
15. Using or attempting to use another person’s user name or password.
16. Posting or plagiarizing work created by another person without his or her consent.
17. Posting anonymous messages or accessing learning games using anonymous user names
18. Using the network for commercial or private advertising.
19. Forging electronic mail messages.
20. Attempting to read, alter, delete, or copy the electronic mail of other system users.
21. Using the school’s computer hardware, network, or Internet link while access privileges are suspended.
22. Using the school’s computer hardware, network, or Internet link in a manner that is inconsistent with a teacher’s directions and generally accepted network etiquette.
23. Attempting to alter the settings and/or configuration of a computer or any of the school’s software. Examples include changing screen colors, backgrounds, screen savers, etc.
24. ***Georgia law makes it a felony to change or disrupt a computer or network for any length of time (Georgia - Computer Systems Protection Act of 1991).***

Cyber Bullying

SDCCS considers treats cyber bulling the same as in person bullying. Cyber bullying is when a child is threatened, harassed, humiliated, or embarrassed by another child using digital technologies such as the Internet.

1. Some examples of cyber bullying include
2. Pretending to be someone else online to trick others
3. Spreading lies and rumors about others
4. Tricking people into revealing personal information
5. Sending or forwarding mean text messages
6. Posting pictures of people without their consent

Cyber Safety

All students participate in cyber safety classes each year, with a focus on keeping students safe online. Some of the main points include:

1. Never post or share your personal information online (this includes your full name, address, telephone number, school name, parents’ names, or Social Security number).
2. Never share your passwords with anyone, except your parents.
3. Never meet anyone face to face whom you only know online.

Adoption

This Internet Safety Policy was adopted by the Board of San Diego Cooperative Charter School at a public meeting, following normal public notice, on <April 12, 2022>.

This Internet Safety Policy was adopted/revised by the Board of San Diego Cooperative Charter School at a public meeting, following normal public notice, on <April 12, 2022>.