



Network Use Guidelines

District Procedure 4580 provides information about the privileges and responsibilities of using the Internet and district networks as part of your student's educational experience. The district SanDiNet is an electronic network with access to the Internet.

Students will have access to:

- Electronic mail (e-mail) communication with people all over the world.
- Information, online databases and news from a variety of sources and research institutions.
- District provided software and public domain/shareware software of all types.
- Discussion groups on a wide-variety of topics.
- Variety of web-based and software programs to publish content to the web.
- Collaborative web-based programs for the purpose of project based learning.
- Online courses and curriculum, academic software and electronic learning resources.

1. Responsibilities

San Diego Unified School District has taken reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. "Harmful matter" refers to material that, taken as a whole by the average person applying contemporary statewide standards, describes in an offensive way material that lacks serious literary, artistic, political or scientific value for minors. (Penal Code, section 313)

The teacher and 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. San Diego Unified School District takes no responsibility for the accuracy or quality of information from Internet sources. Use of any information obtained through the Internet is at the user's risk.

2. Acceptable Use

The purpose for schools having access to SanDiNet and the Internet is to enhance teaching and learning by providing access to 21st Century tools and resources as well as online instruction. Use of another organization's data networks (e.g. Cell Phone Carriers) or computing resources must comply with rules of that network as well as District User policies.

3. Prohibited Uses

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

- a. Information that violates or infringes upon the rights of any other person;
- b. Bullying by using information and communication technologies (cyber-bullying);
- c. Defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or illegal material;
- d. Advertisements, solicitations, commercial ventures or political lobbying;
- e. Information that encourages the use of controlled substances or the use of the system for the purpose of inciting crime;
- f. Material that violates copyright laws. (District Procedure 7038)
- g. Vandalism, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited (Penal Code, Section 502).

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

4. Privileges

The use of SanDiNet and the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The administration, teachers and/or staff may request the site system administrator or district security administrator to deny, revoke or suspend specific user access.

5. Network Rules and Etiquette

The use of SanDiNet and the Internet requires that students abide by district rules of network use and etiquette. These include, but are not limited to, the following.

- a. Be polite. Do not send abusive messages to anyone.
- b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Anything pertaining to illegal activities is strictly forbidden.

Note: E-mail and web-based programs are not private and are subject to review by district staff. People who operate the system have access to all mail. Messages relating to, or in support of, illegal activities must be reported to appropriate authorities.

- c. Maintain privacy. Do not reveal the personal address, phone numbers, personal web sites or images of yourself or other persons. Before publishing a student's picture, first name, or work on the Internet, the school must have on file a parent release authorizing publication.
- d. Cyber-bullying is considered harassment. Refer to The Policy Against Harassment & Discrimination.
- e. Respect copyrights. All communications and information accessible via the network are assumed to be the property of the author and should not be reused without his/her permission.
- f. Do not disrupt the network.

6. Cyber-Bullying

Cyberbullying is the use of any electronic communication device to convey a message in any form (text, image, audio, or video) that intimidates, harasses, or is otherwise intended to harm, insult, or humiliate another in a deliberate, repeated, or hostile and unwanted manner. Staff and students will refrain from using personal communication devices or district property to cyber-bully one another. Cyber-bullying may include but is not limited to:

- a. Spreading information or pictures to embarrass;
- b. Heated unequal argument online that includes making rude, insulting or vulgar remarks;
- c. Isolating an individual from his or her peer group;
- d. Using someone else's screen name and pretending to be that person;
- e. Forwarding information or pictures meant to be private.

7. Security

Security on any computer system is a high priority. If you feel you can identify a security problem on SanDiNet, notify the district Educational Technology Department or the Information Technology Department either in person, in writing, or via the network. Do 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 access to SanDiNet and the Internet.

8. Vandalism

Vandalism will result in cancellation of privileges. This includes, but is not limited to, the uploading or creation of computer viruses.