SAN DIEGO UNIFIED SCHOOL DISTRICT NETWORK USE GUIDELINES

Reference: Administrative Procedure 4580

Please read the following carefully. This will give you information about the privileges and responsibilities of using the Internet and district networks as part of your student's educational experience. The district's network provides access to the Internet.

Students have access to:

- Information, online databases and news from a variety of sources and research institutions.
- District provided software and public domain-shareware software of all types.
- 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.
- Electronic mail (e-mail) to access learning resources.
- Discussion groups on a wide variety of topics.

I. **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/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.

II. **Acceptable Use**. The purpose of schools having access to district networks 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.

III. **Prohibited Uses**. Transmission of any material in violation of any federal, state or 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 (cyberbullying).
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 Administrative 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.

IV. **Privileges**. The use of district networks 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.

V. **Network Rules and Etiquette**. The use of district networks 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. In all messages, do not swear or use vulgarities or any other inappropriate language. Note: E-mail and web-based programs are not private and are subject to review by district staff. System operators 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 or phone numbers, personal websites 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. Cyberbullying is considered harassment. (Refer to the policies against Discrimination and Harassment in the Facts for Parents handbook, Section A, available on the district website.)
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. Do not use the network in a way that would disrupt the use of the network by others.

VI. **Cyberbullying**. Cyberbullying is the use of any electronic communication device to convey a message in any form (e.g. 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. Using personal communication devices or district property to cyberbully someone is strictly prohibited and may result in the cancellation of network privileges and/or disciplinary action. Cyberbullying may also include but is not limited to:

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

VII. **Security**. Security on any computer system is a high priority. If you feel you can identify a security problem on district networks, you must notify the Integrated Technology Support Services (ITSS) 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 district networks and the Internet.

VIII. **Vandalism**. Vandalism will result in cancellation of privileges. This includes, but is not limited to, the uploading or creation of computer viruses. Cellular Telephone and Electronic Signaling Device Policy. Education Code section 48901.5 allows school boards to set policy on the use and possession of cellular telephones and other electronic signaling devices on school campuses. Board of Education Policy H-6980 allows student possession and use of cellular phones, pagers, and other electronic signaling devices on school campuses and school buses, at school-sponsored activities, and while under supervision and control of district employees under the following circumstances:

* All students (K-12) may use these devices on campus before school begins and after school ends.
* Students in high school, grades 9-12, may use them during the lunch period.
* The devices must be kept out of sight and turned off during the instructional program and in the classroom.
* Unauthorized use is grounds for confiscation of the device by school officials, including classroom teachers.

Repeated unauthorized use of such devices may lead to disciplinary action.

District Procedure: 4580 (Effective: 4/18/95; Revised: 11/15/13)