SAN DIEGO CITY SCHOOLS
Network Use Guidelines

Reference: District Administrative Procedure 7039

Please read the following carefully. This will give you information about the privileges and responsibilities of using the Internet and district networks.

The district's network provides access to the Internet. The Internet is an electronic highway connecting thousands of computers all over the world.

Staff will have access to:

- Electronic mail (e-mail) communication with people all over the world.

- Information and news from a variety of sources and research institutions.

- Public domain and shareware software of all types.

- Discussion groups on a wide variety of topics.

- And many more.

I.   **Responsibilities.** San Diego City Schools has taken reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. However, on a public network it is impossible to control all materials. "Harmful matter" means matter that, taken as a whole by the average person applying contemporary statewide standards, describes in a patently offensive way material which 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 City Schools 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/sites having access to district networks and the Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. The use of district networks must be in support of education and research and consistent with the educational objectives of San Diego City Schools. Use of another organization's networks or computing resources must comply with rules appropriate for that network.

III.   **Prohibited Use.** Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to, the distribution of:

   a.   Any information that violates or infringes upon the rights of any other person.

   b.   Any defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.

   c.   Advertisements, solicitations, commercial ventures, or political lobbying.

   d.   Any information that encourages the use of controlled substances or the use of the system for the purpose of inciting crime.

   e.   Any material that violates copyright laws, e.g., illegal downloading, reproduction, and distribution of pirated or unlicensed copyrighted computer programs, music, or movie files (District Administrative Procedure 7038).

Any 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 a 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.   **Netiquette (Network Etiquette).** The use of district networks and the Internet requires adherence to rules of network 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. Anything pertaining to illegal activities is strictly forbidden. (**Note**: E-mail is not guaranteed to be private. People who operate the system do 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 of yourself or other persons.

  d.   *Respect copyrights*. All communications and information accessible via the network should be assumed to be the property of the author and should not be reused without his/her permission.

  e.   *Do not disrupt the network*. Do not use the network in a way that would disrupt the use of the network by others.

VI.   **Security.** Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on district networks, you must notify the security administrator at the Information Technology Department of San Diego City Schools 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.

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