ADMINISTRATIVE PROCEDURE

CATEGORY: **Personnel, Staff Ethics**

SUBJECT: **Staff Use of District Data Communications and the Internet**

1. PURPOSE AND SCOPE

1. To outline rules governing district staff's use of district data communications networks and the Internet.

2. **Related Procedures:**
Copying and use of copyrighted materials……7038
Integrated Technology Support Services security of information…….. 5700
Written communications…….....1600

2. LEGAL AND POLICY BASIS

1. **Reference:** Board Policy G–7500; Education Code Section 51870.5; California Penal Code Sections 313, 502.

2. **Access to Harmful Matter.** School districts that provide pupils with access to the Internet or to an online service are required by Education Code section 51870.5 to adopt a policy regarding access to sites that contain or make reference to harmful matter as defined in subdivision (a) of section 313 of the Penal Code. "Harmful matter" means matter that, taken as a whole, the predominant appeal of which to the average person, applying contemporary standards, is to prurient interest (i.e., a shameful or morbid interest in nudity, sex, or excretion); matter which taken as a whole goes substantially beyond customary limits of candor in description or representation of such matters; and matter which taken as a whole is utterly without redeeming social importance for minors.

3. GENERAL

1. **Originating Office.** Questions and suggestions concerning this procedure should be directed to the Integrated Technology Support Services Department.

2. **Definitions**

   a. **Network**: Two or more computer systems linked to allow communication. The district's network connects schools and support offices to provide data communications, such as e-mail, file sharing, and Internet access.

   b. **Internet**: A global network of interconnected computers.

   c. **World Wide Web**: A global, hypertext-based information system accessible through the Internet via HTTP protocol.

d. **Universal Resource Locator (URL)**: The address of a source of information on the Internet.

e. **District E-mail**: Electronic mail messaging over the district's communications networks. (sandi.net electronic mail accounts.)

f. **Personal E-mail**: Electronic mail messaging sent using accounts other than one's assigned, sandi.net email account.

g. **File server**: A shared computer providing data storage and services to users.

h. **District data**: Information maintained and processed in the conduct of district business as required by state or federal mandate and/or district procedure. Confidentiality restrictions may apply to information maintained as district data records and to all copies of those records.

i. **System administrator**: Person(s) responsible for providing and/or managing network services (e.g., file servers, e-mail, Internet services).

j. **Security administrator**: Person(s) responsible for providing network security.

k. **Network use guidelines**: District guidelines for staff regarding acceptable use of the Internet and district networks.

3. **Acceptable Use.** The use of San Diego Unified School District's network services is a privilege and is to be limited to district business as authorized by board policy. Use of the district's network services by district employees should support district policy and procedure in the performance of assigned duties.

a. **Access to certain data and processes** may be allowed through the use of a username and password. Use of an employee's specific username and password is affected in order to assign direct responsibility for work performed while using the username and password to that specific employee.

b. **By accessing district resources and data** through the use of a username and password, the employee agrees to maintain the confidentiality of the username and password. The employee is solely responsible for maintaining the confidentiality of any username and password and shall not request or use another employee's password that has been chosen or is chosen on his or her behalf. The security administrator at the Integrated Technology Support Services is to be informed of any breaches to this procedure.

4. **Prohibited Use**

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

(1) Any information that violates or infringes upon the rights of any other person.

(2) Any defamatory, inappropriate, abusive, inflammatory, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material. Do not use language that would not be appropriate in an educational setting.

(3) Advertisements, solicitations, commercial ventures, or political lobbying.

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

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

b. **Any vandalism**, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited (California Penal Code section 502).

Cyber-Bullying, 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 is strictly prohibited. Using personal communication devices or district property to cyber-bully one another may result in the cancellation of network privileges and /or disciplinary action. Cyber-bullying may include but is not limited to:

(1) Spreading information or pictures to embarrass;

(2) Heated unequal argument online that includes making rude, insulting or vulgar remarks;

(3) Isolating an individual from his or her peer group;

(4) Using someone else's screen name and pretending to be that person;

(5) Forwarding information or pictures meant to be private.

Warning: The district reserves the right to monitor all network activity. No employee should have any expectation of privacy as to his/her usage. The district reserves the right to inspect any and all files on computers or servers connected to the district's network.

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

d. **Legal Issues.** The district is not responsible for an employee's use of e-mail that breaks the law. All email and calendar items sent or received in the district email system are archived and subject to disclosure under public records law and eDiscovery. Sending confidential information to unauthorized people is prohibited. Because email is increasingly being used in litigation, always keep in mind:

(1) Every email you write is likely to be preserved by somebody, somewhere.

(2) Email can be misinterpreted in court cases: write clearly and unambiguously.

(3) All messages should uphold the ethical values of the District.

5. **District E-mail.** Users of electronic mail systems should not consider electronic communications to be either private or secure; such communications are subject to public records law and eDiscovery. Messages relating to or in support of illegal activities must be reported to appropriate authorities. Other conditions for use include, but are not limited to, the following:

a. **Individuals are to identify** themselves accurately and honestly in e-mail communications. E-mail addresses may not be altered to impersonate another individual or to create a false identity.

b. **The district retains the copyright** to any material deemed to be district data. Use of district data sent as e-mail messages or as enclosures will be in accordance with copyright law and district standards.

6. **Personal E-mail.** When accessed through the district's network, employees have no expectation of privacy to their personal emails. Regardless of whether the district's network is used to access personal email, any communication, including those from a personal email account, when acting in your official, district capacity, becomes public record. As such, employees are explicitly responsible for using only district email

and district-approved communication services to conduct district business. Personal communication shall not interfere with work responsibilities. Do not auto-forward business email to personal email accounts.

7. **Responsibilities** – **Reasonable precautions by district staff**. San Diego Unified School District maintains reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. 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. However, staff should understand that on a public network it is not possible to control *all* material and will accept responsibility for complying with district procedures and with standards of acceptable use.

8. **Security.** Security on any computer system is a high priority, especially when the system involves many users. If any user identifies a security problem with district networks, he/she must notify the security administrator at the Integrated Technology Support Services, either in person, in writing, or via the network. Users should *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 network privileges. Violations include, but are not limited to:

    a. **Illicitly gaining entry**, or "hacking," into a computer system or obtaining account passwords.

    b. **Intentionally creating** or distributing a computer virus.

    c. **Using district systems or equipment** or knowingly disable or overload any computer system or network or to circumvent the security of a computer system.

    d. **Knowingly bypassing** a district "firewall" used for blocking inappropriate Internet sites and for security screening. Said "firewall" may only be bypassed during use by an adult and to enable access for a bona fide district research purpose.

9. **District Web Standards.** District websites must be in compliance with the requirements set forth in *SDUSD Web Standards* (attachment 2). District related social networking sites must comply with the district's social networking guidelines and procedure.

4. IMPLEMENTATION

5. FORMS AND AUXILIARY REFERENCES

1. Network Use Guidelines, Attachment
2. San Diego Unified School District Web Standards, Attachment

6. REPORTS AND RECORDS

7. APPROVED BY

Lawrence M. Schoenke

General Counsel, Legal Services
As to form and legality

8. ISSUED BY

Chief of Staff