SCHOOL DISTRICT

EMPLOYEE ACCEPTABLE USE POLICY FOR DISTRICT COMPUTERS, ELECTRONIC DEVICES, NETWORK AND OTHER ELECTRONIC INFORMATION RESOURCES

School District recognizes that electronic information resources can enhance productivity, facilitate professional communication, and assist in providing quality educational programs. This policy applies to, and describes the responsibilities and obligations of, all District employees using the District's electronic information resources, including the District's computers, electronic devices, and network.

1. Description of the District's Electronic Information Resources. The District's electronic information resources covered by this policy include the District's computers, electronic devices, and network.

a. Definition of "District Computer":

The term "District computer" means any computer, including a laptop computer, that is owned, leased or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by the District from another agency, company or entity, whether or not the computer is equipped with a modem or communication peripheral capable of digital connection.

b. Definition of "District Electronic Device":

The term "District electronic device" means any device other than a District computer that is capable of transmitting, receiving, or storing digital media and is owned, leased, or rented by the District, purchased with funds from a grant approved by or awarded to the District, or borrowed by the District from another agency, company or entity, whether or not the electronic device is portable and whether or not the electronic device is equipped with a modem or other communication peripheral capable of digital connection.

District electronic devices include but are not limited to:

- ♦ telephones;
- ♦ cellular telephones;
- ♦ radios;
- ♦ pagers;
- ♦ voice mail;
- ♦ e-mail;

- ♦ text messages;
- ♦ digital cameras;
- ♦ personal digital assistants such as Palm Pilots and Smart Phones;
- ♦ portable storage devices such as thumb drives and zip drives;
- ♦ portable media devices such as IPODs and MP3 players;
- ♦ optical storage media such as compact discs (CDs) and digital versatile discs (DVDs);
- ♦ printers and copiers;
- ♦ fax machines.

c. Definition of "District Electronic Network":

The term "District electronic network" means the District's Local Area, District-wide, and Internet systems, including software, e-mail and voice mail systems.

2. Ownership. The District's electronic information resources, including District laptop computers and portable electronic devices, are District property, provided to meet District needs. They do not belong to employees.

All District computers and electronic devices, including District laptop computers and portable electronic devices, are to be registered to the District, and not to the employee. All software on District computers and electronic devices, including District laptop computers and portable electronic devices, is to be registered to the District, and not to the employee, except as provided in Section 6.

No employee shall remove a District computer or electronic device from District property without the prior, express authorization of .

The use of District electronic information resources is a privilege which the District may revoke or restrict at any time without prior notice to the employee.

3. No Employee Privacy. Employees have no privacy whatsoever in their personal or work-related use of the District's computers, electronic devices, network, and other electronic information resources, or to any communications or other information in the District's electronic information resources or that may pass through District electronic information resources. The District retains the right, with or without cause, and with or without notice to the employee, to remotely monitor, physically inspect, or examine the District's computers, electronic devices, network, or other electronic information resources, and any communication or information stored on or passing through the District's electronic information resources, including but not limited to software, data and image files, Internet use, e-mails, text messages, and voice mail.

When an employee leaves the employment of the District, management shall be given access to, and the authority to dispose of, any and all of his or her computer files, e-mail, voice mail, text messages, and any other electronically stored information.

4. Personal Use. Employees shall use the District's computers, electronic devices, network, and other electronic information resources primarily for purposes related to their employment. District laptop computers and portable electronic devices shall be used solely by authorized employees, and not by family members or other unauthorized persons.

Where approved by in advance, an employee may make minimal personal use of District electronic information resources as long as such use does not violate this policy, does not result in any additional fee or charge to the District, and does not interfere with the District's normal business practices or the performance of an employee's duties. As described in Section 3, employees have no privacy whatsoever in their personal use of the District's computers, electronic devices, and network, including but not limited to software, data and image files, Internet use, text messages, and e-mails.

5. Password Protection. To protect against unauthorized use, all District computers and electronic devices, including laptop computers, that are capable of being password protected, shall be password protected, even if a computer or electronic device is assigned to a single employee for his or her sole use. If password protection is not technically feasible, the employee to whom the computer or electronic device is assigned shall be responsible for physically protecting it against unauthorized use. A screen saver which is capable of being password protected shall be password protected.

Each employee shall be responsible for registering his or her password(s) with , whether the password protection is at the system level or program level. The District needs the ability to access its own equipment.

6. Software and Electronic Devices. Software, computers, and electronic devices must meet specific standards to protect the District's network and other electronic information resources. In addition, violations of software copyright law have the potential of costing the District millions of dollars.

Therefore, a technology administrator shall be designated at . Only the designated technology administrator at shall be allowed to authorize: 1) the installation, maintenance, or removal of software on District computers and electronic devices; and 2) the connection of non-District electronic devices to District computers.

Unless directed to or authorized by , no employee shall install, maintain, or remove software on District computers and electronic devices. Unless directed to or authorized by , no employee shall connect an electronic device to District computers, whether hardwired or wireless.

is authorized to approve employee requests for the installation of non-District software, subject to the following limitations:

a. Software not [reasonably] related to the mission of the District shall not be installed.

b. No software shall be installed without written proof of licensing, which shall be retained by . Multiple installations of the same license number will be assumed to violate copyright unless a multiple license provision can be demonstrated.

c. The employee shall surrender to the District all rights whatsoever he or she may have in the software, including but not limited to the following:

The District has the right to remove the software at any time and for any reason without prior notice to the employee.

The District has no obligation to return the software to the employee.

If the employee is assigned to a different computer or electronic device, the District has no obligation to install the software on that equipment.

Employees who have been authorized to download and install software shall run the most up-to-date District approved anti-virus software on all files and programs downloaded, and shall adhere to copyrights, trademarks, licenses, and contractual agreements applicable to the software, including provisions prohibiting the duplication of material without proper authorization and the inclusion of copyright notices in any use of the material.

7. Filters and Other Internet Protection Measures. To ensure that the use of the District's network is consistent with the District's mission, the District uses content and bandwidth software to prevent access to pornographic and other websites that are inconsistent with the mission and values of the District. No employee shall bypass or evade, or attempt to bypass or evade, the District's filter system.

8. Other Unacceptable Uses. In addition to the previous requirements, employees using the District's computers, electronic devices or network shall be responsible for using them only in compliance with the following requirements.

a. An employee shall use only his or her assigned account or password to access District computers, electronic devices, and network. No employee shall permit the use of his or her assigned account or password, or use another person's assigned account or password, without the prior express, written consent of .

b. Employees are prohibited from using the District's computers, electronic devices, network and other electronic resources for knowingly transmitting, receiving, or storing any oral or written communication that is obscene, threatening or disruptive, or that reasonably could be construed as harassment or disparagement of others based on their race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, age, or sexual orientation. This prohibition applies to written and oral communication of any kind, including music.

c. Employees are prohibited from using the District's computers, electronic devices and network for knowingly transmitting, receiving, or storing any visual image that depicts actual or simulated torture, bondage, or physical abuse of any human being or other creature, or that is sexually explicit.

   i. "Sexually explicit" includes, but is not limited to depictions of actual or simulated human sex acts, and the unclothed human genitalia, pubic area, anus, buttocks, and female breast that lack serious artistic, literary, scientific, or political value.

   ii. This prohibition applies to visual depictions of any kind, including screen savers, drawings, cartoons and animations.

d. Employees shall not knowingly store or transmit copyrighted material on the District's computers, electronic devices, or network without the permission of the holder of the copyright. Employees shall download copyrighted material only in accordance with applicable copyright laws.

e. Employees are prohibited from knowingly using the District's computers, electronic devices, and network to intentionally access information intended to be private or restricted; change data created or owned by another user or any other agency, company or network; make any unauthorized changes to the appearance or operational characteristics of the District's system; load, upload, download or create a computer virus; alter the file of any other user or entity; or remove, change or add a password without the approval of .

f. Employees are prohibited from remotely accessing any District computer or server without prior express written approval of .

g. Employees are prohibited from uploading to a non-District server any file contained on a District computer or server; whether the file is work related or personal, unless the employee has been granted the prior express written approval of .

h. Any text transmission can only be used by authorized District blog messaging systems and/or device.

i. Employees also are prohibited from using the District's computers, electronic devices, and network for:

i. personal financial gain;

ii. commercial advertising;

iii. political activity as defined in Education Code sections 7050-7058;

iv. religious advocacy;

v. promoting charitable organizations;

vi. communicating in someone else's name;

vii. attempting to breach network security;

viii. creating, sending or receiving materials that are inconsistent with the mission and values of the District;

ix. mass distribution of e-mail to a school site without the prior approval of ;

x. mass distribution of e-mail to the District office without the approval of ;

xi. accessing pornographic or other websites that are inconsistent with the mission and values of the District;

xii. any activity prohibited by law, Board policy or administrative regulations, or the rules of conduct described in the Administrative Code.

9. Violation of This Policy. Technology employees shall promptly report violations of this policy to .

Employees who violate this policy are subject to discipline, up to and including termination, pursuant to the provisions of applicable laws governing employee discipline, and applicable District policies, procedures and collective bargaining agreements. The employee's use of the District's electronic information resources also may be restricted, suspended, or revoked.