

VISTA UNIFIED SCHOOL DISTRICT

All Personnel

Exhibit 4040

EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

Communications and computer technology at Vista Unified School District (VUSD) are provided and maintained for instructional, educational and administrative purposes only. This document implements Board Policy 4040, Employee Use of Technology, and governs the use of technologies by employees during the performance of their duties.

1. ACCESS TO TECHNOLOGY EQUIPMENT AND SERVICES

- 1.1 Access to technology is provided to facilitate the instructional and administrative tasks performed by district employees and volunteers. The level of access provided will coincide with the requirements of each employee's job functions and related collective bargaining agreements.
- 1.2 Computer files and communications over electronic networks, including email, voice mail and Internet access, are not private. This technology should not be used to transmit confidential information about students, employees, or District business.
- 1.3 To ensure proper use, the Superintendent/designee may monitor the District's technological resources, including email, voice mail systems and Internet usage, at any time without advance notice or consent.

2. ACCEPTABLE USE

- 2.1 It is a general policy that online communication is to be used in a responsible, efficient, ethical, and legal manner in support of education, business and/or research and within the educational program and goals of VUSD. The use of electronic information resources is a privilege, not a right. Each user is personally responsible for this provision at all times when using electronic information services.
- 2.2 Administration may set more restrictive guidelines for employees in their area of responsibility.
- 2.3 While electronic information resources offer tremendous opportunities of educational value, they also offer persons with illegal or unethical purposes avenues for reaching students, teachers, and others, including parents. VUSD does not have control of the information on commercial electronic information services or the information on the Internet, although it attempts to provide prudent and available barriers. Sites accessible via the Internet may contain material that is illegal, defamatory, inaccurate or potentially offensive to some people.
- 2.4 Should an employee see any unacceptable materials or inappropriate use, he/she shall notify the site administrator or supervisor immediately. Report any instances where the Acceptable Use Policy or security may be violated. Report inappropriate Internet Web sites to Administration so Information Systems Department (ISD) can block access to the site.
- 2.5 If an employee doubts or questions the appropriate use of a District-provided electronic system, the employee shall review the use in advance with a supervisor.

3. PROPER USE AND CARE

- 3.1 Equipment abuses are unacceptable whether out of frustration, misuse, negligence or carelessness. Users are responsible for damage to or loss of District equipment.

District vandalism policies apply, making users liable for intentionally inflicted damage.

- 3.2 Users should not attempt repairs without authorization or support from designated District or school site personnel. Volunteers – parents, family members, or friends – are not authorized to attempt repairs on District equipment.
- 3.3 Guidelines for the care and use of computer software are similar to hardware policies. Users are responsible for damage to or loss of District software systems. District vandalism policies apply to software as well, making users liable for intentionally inflicted damage.
- 3.4 Users shall not install or modify applications without approval and support of the District Information Systems Department. Any unauthorized changes to systems, operating software, application software, or hardware configurations will be reversed when discovered by ISD staff. File-sharing software cannot be installed or used on District computers for the purpose of illegally sharing copyrighted materials such as music, images and software. This type of software is often used to “pirate”, or illegally copy music across the Internet. The use of this type of software is illegal when used to share copyrighted material. The most common use is the illegal “swapping” of music encoded in the MP3 format and is a violation of U.S. copyright laws.
- 3.5 Users shall not download or install copyrighted software without proper licensing. Non-licensed software will be deleted.
- 3.6 Copyrighted material shall be posted online only in accordance with applicable copyright laws.
- 3.7 In order to ensure proper configuration and to safeguard network security and performance, users should not attach computers, printers, network equipment (including wireless access points), or other types of hardware to the District's network without prior approval and support of the Information Systems Department. Any equipment found to be in violation of this policy will be immediately disconnected and/or have network access blocked.

PERSONAL RESPONSIBILITY

- 4.1 All technology equipment is District property and is provided for instructional or administrative use only. Personal use is limited in the same manner as other similar District property – telephones, copiers, postage, office supplies and instructional materials. Supervisors will provide guidance as to the appropriate level of personal use.
- 4.2 Employees shall not access the system, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.
- 4.3 Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.
- 4.4 Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee. In addition, District electronic resources cannot be used to conduct political or religious activities. District email cannot be used to advertise or solicit for non-district sponsored events, activities, or organizations.

- 4.5 The District maintains a public Internet site and an in-house Intranet site. All materials published on these sites must follow the same Board Policies and Education Code Sections that apply to printed material. These policies include restrictions on the content, nature, purpose, and volume of information to be published. Intranet pages are provided for District employees and students only. Any information to be posted on the public Web site or in-house Intranet site must be approved through Cabinet-level administrators (or their designee). Principals must approve all postings on school web sites. Restrictions apply to links to other sites that may not be appropriate and to personal information or pictures of students without parental consent.
- 4.6 Do not store personal files or applications on District media/ *equipment*.
- 4.7 Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' mail.
- 4.8 Employees shall not develop any classroom or work-related web sites, blogs, forums, or similar online communications representing the District or using District equipment or resources without permission. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.
- 4.9 Users shall report any security problems or misuse of the services to the Superintendent or designee.

5. SECURITY AND PASSWORDS

- 5.1 To maintain security, users are issued unique User ID's and passwords to enable their access. Do not use other people's passwords. Do not write down a password where others can see it, and change passwords regularly as recommended by ~~IS~~ *the Information Systems* Department. Alternative system access measures may be implemented upon authority of the Superintendent.

6. PENALTIES FOR VIOLATIONS

- 6.1 Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow these guidelines may face disciplinary action in accordance with collective bargaining agreements, state law, and Board policy.

7. EMPLOYEE ACKNOWLEDGEMENT

- 7.1 All employees of VUSD will be required to acknowledge that they have received (includes online access), read and accepted this Acceptable Use of Technology Agreement.

VISTA UNIFIED SCHOOL DISTRICT
EMPLOYEE ACCEPTABLE USE OF TECHNOLOGY AGREEMENT
EMPLOYEE ACKNOWLEDGEMENT

I have received (includes online access), read and accept the guidelines in the Board Policy and Administrative Regulation on Employee Acceptable Use of Technology.

Print Name

Signature

Date