Sequoia Union HSD | AR 4040 Personnel

Employee Use Of Technology

The Information Age revolution brings with it a host of new laws that reflect the fast paced change of electronic communication. It is important that staff understand their obligations and responsibilities while using the technological resources of the Sequoia Union High School District in this new environment. The computer, telephone, information, and network resources made available by the District and staff responsibilities and obligations in the use of these resources are described below. All district employees are required to read and sign Exhibit 4040-Technology Use Agreement.

The Superintendent and his staff, specifically the Assistant Superintendent of Human Resources and the Assistant Superintendent of Administrative Services, are responsible for the development, maintenance, and enforcement of this and related board policy. Staff will be informed of updates and changes to board policies and administrative regulations related to the use of the District's technological resources.

Computer and Network Environment

The District has created extensive networks with information, telephone, and computing resources for staff and student use. In addition, the District provides a large and continuously growing number of computer workstations, printers, peripherals, software, training and supplies to all sites. These items are provided to allow staff and students to perform their tasks effectively in meeting the goals and needs for which the District was established. Staff shall receive training in the appropriate use of these items and training will include information regarding web publishing guidelines, copyright laws, etc.

Improper use of any of these resources can cause problems related to the needs of some or all employees and students in the District. Violation of specific local, state, and federal laws referenced later in this document may call for prosecution under the law, including fines and imprisonment. The District may take disciplinary action against employees for misuse of computer, network, and information resources.

Privacy of District Records - Student, Staff, and Business Information

Both student and employee records are protected by various state and federal laws:

State Statutes:

Education Code, Section 67100

Information Practices Act of 1977 (Civil Code Section 1798)

Public Records Act (Government Code Section 6250)

Penal Codes, Section 502

Federal Statutes:

Federal Family Educational Rights and Privacy Act of 1974

Federal Privacy Act of 1974

Electronic Communications Privacy Act of 1986

It is probable that during a staff member's employment with the District, he/she will have access to confidential student, employee, or business information. It is every staff member's responsibility to safeguard this information from unauthorized use or access by unauthorized persons. Staff shall not use personal or confidential information

for his or her own use or personal gain. Staff must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including, but not limited to, voice, electronic (disk file, diskette, CD ROM, magnetic tape, email, or any other memory device), paper, photographic, and microfiche information. Included under this precaution is the disposal of any privacy-related materials.

Ownership

It must be understood that the District's business information, telephone network, computer, and software resources, peripherals, and supplies are district property, provided to meet District needs. They do not belong to individuals, but are only made available for the purposes required by staff while employed by the District.

Employees shall be responsible for the appropriate use of technology and shall use the District's technological resources only for purposes related to their employment, except for occasional, infrequent personal use that does not interfere with the operations/business of the District.

Use of Telephones, Mobile Phones, and Voicemail

Telephones and mobile phones are provided to conduct the business of the District. In many cases, voice mail is also provided. These services are intended to provide a means of communication for employees to contact parents and students, agencies, vendors, other institutions, and government officials. When using these services, staff must always reflect a businesslike and professional demeanor. District phones may be used for occasional, infrequent personal use that does not interfere with the operations/business of the District. A staff member is prohibited from making personal calls that incur long distance charges.

Use of Personally-Owned Software or Equipment

The District attempts to ensure that all hardware and software meet specific standards which will operate without causing disruption of the District's computer and network resources. Therefore, the regular use of personally-owned computer hardware, is not permitted, except when authorized by the Assistant Superintendent of Administrative Services or designee.

Software Copyright Law

Violations of copyright law have the potential of costing the District millions of dollars. Staff members are prohibited from installing any software without having proof of licensing. Staff may not install software licensed for one workstation on multiple machines. Staff should be aware that if, for example, a new workstation is purchased, new software licenses for the software to be installed on it must also be purchased. If the computer being replaced will be retired from use, the software may be removed from it and transferred to a new workstation.

Online/Internet Services: User Obligations and Responsibilities

The Internet provides an extremely valuable resource for learning and communicating with people throughout the world. It can be a marvelous tool to enhance student and staff education and productivity. Unfortunately, the Internet also contains a large amount of information that is inappropriate for use in an educational environment.

Employees are authorized to use District equipment to access the Internet or other online services in accordance with the Board policies and administrative regulations related to the use of the District's technological resources.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under the account number to which they have been assigned.

2. Employees shall use the system safely, responsibly, and primarily for work-related purposes. While it is hoped that employees will enjoy the use of Internet resources, it must be emphasized that these resources are provided at district expense to enhance job function and maximize job effectiveness. Private or personal non-commercial

use of the Internet is permitted as long as it is consistent with Board policies, administrative regulations, and any applicable laws, and is limited to occasional, infrequent use that does not interfere with the District's normal business practices and performance of the individual's task.

3. Employees shall not access, post, submit, publish, or display harmful or inappropriate matter, including material 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.

(cf. 4030 - Nondiscrimination in Employment)

(cf. 4031 - Complaints Concerning Discrimination in Employment)

(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations. It is imperative that employees not use the Internet in such a way as to bring civil or criminal liability or public reproach upon the District.

(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)

5. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Materials obtained from the Internet that are copyrighted, with proper citation, and with limited educational use, may be posted online under the Principle of Fair Use as contained in U.S. Copyright law. These materials may not be redistributed on the Internet or in any other manner without written consent of the copyright owner or as prohibited by law. Materials are protected by copyright whether they bear copyright information or not.

(cf. 6162.6 - Use of Copyrighted Materials)

6. 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' email.

7. 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 of the Superintendent or designee. 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 over which it has control or to which it has access.

(cf. 1113 - District and School Web Sites)

8. Users shall report any security problem or misuse of the services to the Superintendent or designee.

To be in compliance with E-rate regulations and the Children's Internet Protection Act (CIPA), the Sequoia Union High School District has an effective filter in place. The purpose of this filter is to limit users from visiting inappropriate web-sites. The District is aware that the filter may block educational related sites. If a teacher needs a site unblocked, he or she must contact Technology and Information Services to review the request and unblock the site.

Misuse of Computer Resources

The computing resources of the District are used by thousands of students and employees. In order to ensure that these resources are available and working properly, personal use of these resources must not negatively impact others.

For example, staff and students may not break into computer systems or those resources to which authorization has not been granted. Staff may not attempt to maliciously alter, erase, damage, destroy, or make otherwise unusable or inaccessible any data, software, computer, or network system. Attempts or actions of this nature are unlawful and may result in any combination of disciplinary action and/or prosecution and fines, including litigation costs and payment of damages under applicable local, state, and federal statutes.

Individual Computer Account

In order to utilize the District's computer and network resources, staff will be assigned an "user ID" and password. Based on position and supervisor's authorization, staff may be provided with access levels which permit the viewing, creating, altering, deleting, printing, and transmitting of information.

All technologies, communications, and, in general any files or electronic information are not private, and, therefore, the Superintendent or designee may monitor the use of any technology or examine any electronic system at any time without advance notice or consent

Staff is responsible for maintaining the security of personal accounts and may not release it for use by any other individual. Staff must accord the user account the same significance as a hand-written signature. Failure to do so by releasing this information to another individual may be considered failure to safeguard District property and result in disciplinary action.

Therefore, it is extremely important that staff use a password that cannot be guessed by others through personal knowledge. Users shall take all precautions to protect their passwords. They shall not release password to any unauthorized persons, and, at the same time, they shall make sure their immediate supervisor has the password. Technology and Information Services must be contacted if it is suspected someone else may have accessed a personal account. It is a simple matter to change a password, but it may take days to reconstruct damaged records or a computer system if someone breaks into a personal account. Staff is encouraged to periodically change passwords of personal accounts.

A staff member should never leave his or her workstation unattended while signed on to any account; doing so allows others to sit at the workstation and, using personal rights and privileges, perform destructive acts. This has been the most common method used in the past for students to make changes to their own and others records.

Under certain circumstances, user IDs and passwords may be shared by a group of employees when doing so makes information access convenient with a minimum of administrative overhead. Examples include District-subscribed online services that teachers may wish to access from outside of the District network. Group IDs and passwords should be held in confidence and never shared with students. If staff suspects that the security of such information has been compromised, the network administrator must be notified at once.

Only employees may have direct publishing (write privilege) access to District web, mail, and list servers. Those who assume responsibility for posting student work must never delegate this responsibility to students. Passwords are not to be stored where students may have access to them. Passwords are to be periodically changed.

Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, and other damaging programs that attack computer and network resources. The District attempts to maintain anti-virus software in order to minimize the impact of these viruses, but it is each staff member's responsibility to take precautions to protect his or her computer and all others throughout the District.

For example, staff must avoid opening email attachments from unknown individuals. If someone unknown to staff sends an attachment, staff must contact him or her and verify what the purpose of the attachment is. Staff members must ensure there are no viruses that may have invaded their attachment.

Likewise, staff members may not download any software from the Internet unless directed to and authorized by a supervisor or the Technology & Information Services department or designee. A staff member may not share any downloaded software with others until they have verified that it does not harbor viruses.

Electronic Mail

The District encourages the use of electronic mail (email) to enhance communication and business activities. Users of this service need to be aware, however, that this technology is still developing, and policies like this one are necessary to ensure appropriate use and to prevent or limit disruptions to work activity and computer services. It is appropriate for the teacher's union to use the email system for official union business.

Cautions About The Use Of Electronic Mail

The nature of electronic mail at this date makes it susceptible to misuse. Users need to be aware that sensitive or private information can be easily forwarded to other individuals that

the originator never intended, both within the District as well as externally throughout the world.

In addition, while email accounts may be password protected, it is up to the individual user to ensure that a password is set and that the password is one that cannot be easily guessed or "hacked."

Because of backup procedures in force with the District's computer services, the fact that an email message was "deleted" does not necessarily mean it cannot be retrieved.

Users of the District's email services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All emails sent and received by individuals through District employee accounts are the property of the District and may be requested by the supervisor and examined when deemed necessary by the Superintendent or the Assistant Superintendent of Human Resources to evaluate and ensure compliance with board policies, administrative regulations, and any applicable laws.

While the District does not have the time or inclination to monitor or read individual email messages, in the event questionable or inappropriate use is suspected or known, such email may be examined and may be cause for disciplinary action ranging from revoking the email account to termination of employment. Users should be aware that in the general course of business, system administrators and email operators may require observation of messages in order to verify system operation.

Email - Personal Use

Private, non-commercial use of the District's email is permissible for occasional, infrequent personal use that does not interfere with the operations/business of the District. Individuals should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace. Each email account is the property of the Sequoia Union High School District. Staff use is a privilege that is revocable.

Email - State, Federal, and Copyright Laws

In addition to this policy, use of the District's email services is subject to all applicable federal and state communications and privacy laws. In particular, users need to be aware that attaching programs, sound, video, and images to email messages may violate copyright laws, and data files containing employee and/or student information is subject to all privacy laws.

Email Restrictions

* Electronic mail may not be used for:

* Unlawful activities

* Commercial purposes

* Personal financial gain

* Use that violates this administrative regulation, related District policies, or other state and federal policies

* Any form of harassment

* Chain letters, sending or forwarding

* Personal fund-raising

* Any other use that interferes with computing facilities and services of the District or its employees

* Spam mail, that is, to exploit list servers or other broadcast systems that amplify widespread distribution of unsolicited email

* Mail bombs, that is, to resend the same email repeatedly to one or more recipients with the intent to interfere with the recipient's use of email

* The District bulletin board, found on the Insider (http://insider) is the appropriate location for posting items such as rooms for rent or items for sale.

Email and Representation

Users shall not give impression that they are representing, giving opinions or otherwise making statements on behalf of the District unless they are appropriately authorized, explicitly or implicitly, to do so. Where appropriate and based on context, an appropriate disclaimer would be, "These are my own statements and views and do not represent those of the Sequoia Union High School District."

Email - False Identity

Employees shall not employ a false identity in sending email or alter forwarded mail out of the context of its original meaning.

Email - Misuse of Computing Services

Email services shall not be used for a purpose that could reasonably be expected to cause, either directly or indirectly, excessive strain on District computing facilities or cause interference with others' use of email, email systems, or any computing facility or services. For example, attaching large files over one megabyte and sending this to multiple users or repeatedly to the same user is a violation of this policy.

Email - Security and Confidentiality

The confidentiality of electronic mail cannot be assured. Users should exercise extreme caution in using email to communicate confidential or sensitive material.

Email - Archiving and Retention

The District maintains an ongoing backup schedule of computer data in order to ensure that these facilities may be restored to use in the event of damage and/or destruction. Because of this practice, email may be stored on backup media for extended lengths of time. Messages that a user assumes to be deleted may be able to be restored if demanded by the appropriate District authority.

Each user should consider whether they want to archive their personal messages to their workstation's hard drive or other disk media on some sort of regular basis, as there is always the possibility that the information may be

lost due to software or hardware problems. The District has systems in place for the length of time email is retained online. This schedule is 180 days for current email. While the District maintains a backup of most email, it is not feasible nor District practice to restore lost or damaged email.

Regulation SEQUOIA UNION HIGH SCHOOL DISTRICT

approved: December 10, 1997 Redwood City, California

revised: January 15, 2003

approved: January 16, 2013