Introduction

The Governing Board recognizes that technology can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing a quality instructional program, and facilitating operations. The Board expects all employees to learn to use the available electronic resources that will assist them in their jobs. As needed, staff shall receive training in the appropriate use of these resources.

Encountering Controversial Material

With accessibility to global computer databases, computer users may encounter material on a database or mail system that is controversial and which users, teachers or administrators, may consider inappropriate or offensive. It is the user's responsibility not to initiate access to such material. The district shall employ filtering/blocking technology to ensure that students may not access inappropriate materials. Employees supervising pupils, as well as employees who may observe students accessing the Internet, are expected to report to the Department of Information Technology instances in which pupils have accessed inappropriate materials online, including, but not limited to, visual depictions of material that is (1) obscene, (2) child pornography, and/or (3) harmful to minors. Also, teachers and other employees whom pupils have informed of instances in which inappropriate materials were accessed should immediately report the information received to the Department of Information Technology.

Privileges and Rights

Lemon Grove School District employees shall be required to sign an agreement on the acceptable use of technology indicating their understanding of this regulation and Board Policy 4040 prior to having the right to access the district's network. The form of this agreement is set forth as Exhibit 4040 to this regulation. Lemon Grove School District computer users have certain network privileges and rights, including:

1. The district's computer systems and other technical resources, including any voice mail or e-mail systems, are provided for use in the pursuit of educational purposes and the district's business and are to be reviewed, monitored, and used only in that pursuit, except as provided in this policy. As a result, computer data, voice mail, and e-mail are readily available to numerous persons. When using the district's computer system, the user's work may be subject to the investigation, search, and review of others in accordance with this policy. In addition, any electronically stored communications that are either sent or received from others may be retrieved and reviewed where such investigation serves the legitimate business and education interest and obligations of the district.

2. Employees of the district are permitted to use the district's computer equipment for occasional, non-district purposes with permission from their direct supervisor. Nevertheless, the employee has no right of privacy as to any information or file maintained in or on the district's property or transmitted or stored through the district's computer systems, voice mail, e-mail, or other technical resources. For purposes of inspecting, investigating, or searching employee's or student's computerized files or transmissions, voice mail, or e-mail, the district may override any applicable passwords or codes in accordance with the best interests of the district, its employees, or its students.

3. Unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the district, or improper use of information obtained by unauthorized means, may be grounds for disciplinary action.

4. Any computer user who received threatening or unwelcome communications should bring them to the attention of

the system administrator or supervisor. Given the scope of data on the Internet, individual computer users must not access data known to be unauthorized.

5. Employees have the right to exercise the freedom of speech and press with regard to computer network and usage. However, this policy prohibits using the network to send any data or materials that are obscene, libelous, or slanderous according to current legal definitions.

6. Applicable district policies and requirements apply to computer network usage and communication. Additionally, the district does not endorse any opinions stated on the network, and any statement of personal belief is implicitly understood to be representative of the author's individual point of view.

Responsibilities

1. The district employs filtering/blocking technology to ensure that minors using the district's system are not exposed to inappropriate materials, including, but not limited to, visual depictions of material that is (1) obscene, (2) child pornography, and/or (3) harmful to minors. Since filters/blocking devises may not provide one hundred percent blocking of inappropriate materials, it is the employee's responsibility to visually monitor student use of the Internet in the classroom or whenever supervising pupils using computers. The employee should encourage students to report instances in which inappropriate materials have been accessed through the district's network. It is the employee's responsibility immediately to report to the Department of Information Technology instances in which the employee has observed or students have reported that blocking/filtering has failed so that the Technology Department can take the appropriate corrective actions.

2. The employee in whose name network account is issued is responsible for its proper use at all times. They shall use the system only under their own account number.

3. Users shall not use the system to promote unethical practices or any activity prohibited by law or district policy.

4. Users shall not transmit material that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

5. Copyrighted material may not be placed on the system without the author's permission. Users may download copyrighted material for their own use only and only in accordance with copyright laws.

6. Vandalism will result in the cancellation of user privileges. Vandalism includes uploading, downloading, or creating computer viruses, and/or any malicious attempt to harm or destroy district equipment or materials or the data of any other user.

7. Users shall not read other users' mail or files; they shall not attempt to interfere with other users' ability to send or receive electronic mail; nor shall they attempt to read, delete, copy, modify, or forge other users' mail.

8. Users are encouraged to keep messages brief.

9. Users shall report any security problem or misuse of the network to the Superintendent or designee.

Prohibitions

1. Using the network for sending and receiving excessive numbers of personal messages

2. Using the network for financial gain or commercial activity

3. Using the network to invade employee privacy rights

4. Impersonating another person in computer communications

5. Changing computer files that do not belong to the user without authorization

6. Placing unapproved software on a computer

7. Transmission of any material in violation of any United States or state regulation, including copyrighted material, threatening, or obscene material

8. Using the network for commercial activities or product advertisement

9. Using the computer network to purchase products, services, or any other item without following district purchase order procedures

10. Removal of computer equipment from school campuses or district or school offices without the authorization of the system administrator

11. Misrepresentation of a computer user's identity

12. Using the computer network to annoy, harass, or invade the privacy of another person

Security

The security of the computer network is crucial. Should a user become aware of a network security problem, the employee shall immediately report this problem to the Director of Information Systems, who serves as the computer system administrator.

Software Licensing

Properly licensed software, only, shall be installed on district computers. Employees are required to strictly follow installation procedures outlined in employee handbooks. Employees shall be held financially responsible for any legal action taken when software copyright has been violated.
LEMON GROVE SCHOOL DISTRICT

Legal Reference:
EDUCATION CODE
51870-51874 Education Technology
GOVERNMENT CODE
3543.1 Rights of employee organizations
PENAL CODE
632 Eavesdropping on or recording confidential communications
UNITED STATES CODE, TITLE 20
6801-7005 Technology for Education Act of 1994
47 United States Code section 254 “Children’s Internet Protection Act” and FCC Rules governing CIPA (FCC 01-120, Released April 5, 2001)

Issued: 5/23/00
Revised: 9/25/01