

SECTION:

TITLE: INTERNET USE BY
EMPLOYEES

ADOPTED: 3/19/97

REVISED: 02/21/2007

CALIFORNIA AREA SCHOOL DISTRICT

1. Purpose

- A. The California Area School District supports use of the Internet and other computer networks for instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.
- B. Internet users are expected to use the Internet and World Wide Web as an educational resource. The Internet and World Wide Web have been available in the school as a resource to promote and enhance the educational experience. All school Internet and World Wide Web resources must be used appropriately and explicitly for instructional and educational purposes only.
- C. For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the School as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
- D. As a public school entity receiving federal funds, this policy is also required for purposes of complying with the Child Internet Protections Act (CIPA) and regulations adopted by the Federal Communications Commission (FCC).

2. Guidelines

II. DISCLAIMER

- A. The electronic information available to students and staff does not imply endorsement by the School District of the content, nor does the School District guarantee the accuracy of information received.
- B. The School District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is received via the Internet.
- C. The School District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

III. NO EXPECTATION OF PRIVACY

- A. There is no expectation of privacy for any user of the California Area School District's computer network, including Internet access and e-mail.
- B. Users shall have no expectation of privacy in anything created, stored, sent or received on a school computer.
- C. California Area retains the right, but not the duty, to randomly or specifically monitor without prior notice any person's use to ensure that the computer network is being used properly, to ensure that it is used in compliance with CIPA, to prevent waste and misuse, for purposes of maintenance, and/or with reasonable cause to suspect misuse of the computer network. This monitoring includes accessing files and communication.
- D. The School District reserves the right to log network use and to monitor fileserver space utilization by School District users.

IV. PRIVILEGE/NOT A RIGHT

- A. The School District establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use may result in cancellation of those privileges and/or appropriate disciplinary action.

V. CIPA COMPLIANCE

- A. The School District establishes that any information that is obscene, child pornographic or harmful to minors, all as defined by the Child Internet Protections Act (CIPA), is inappropriate for access by minors.

B. The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the School's computers are being used for purposes prohibited by law or this Policy. The procedure shall include but not be limited to:

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the School Board.
2. Maintaining and securing a usage log.
3. Monitoring online activities of minors.

VI. DELEGATION OF RESPONSIBILITY

A. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

B. The Superintendent shall have the authority to determine what is inappropriate use.

VII. PROHIBITIONS

A. All users are expected to act in a responsible, ethical and legal manner in accordance with School policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Unlawful activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, threats, obscenity, harassing, and offensive or inflammatory communication.

6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Accessing, downloading or distributing to obscene or pornographic material or child pornography.
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
14. Loading or using of unauthorized games, programs, files, hacking tools, system utilities, music CDs, or other electronic media.
15. Disrupting the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and files (i.e. hacking).
17. Use of the Internet to attack, hack, or otherwise compromise California Area School District's or other computer systems on the Internet is strictly forbidden.

18. Quoting of personal communications in a public forum without the original author's prior consent.
19. Unauthorized disclosure, use and dissemination of personal information regarding minors.
20. Chatting, chat rooms, and the use of chat services not authorized by the School District are strictly prohibited. This includes but is not limited to AOL Instant Messenger, Hotmail and other of this type.
21. The Use of E-Mail service provided by California Area School District is for educational purposes only. All communications are to be for approved educational purposes only. Using E-mail provided by services other than California Area School District is strictly prohibited. This includes but is not limited to Hotmail, Yahoo Mail, Lycos Mail and other third party mail retrieval services.

B. Student users shall not use electronic mail (e-mail) without receiving specific authorization from a teacher or Administrator

C. General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

VIII. SECURITY

A. System security may be protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or School files. To protect the integrity of the system, the following guidelines shall be followed:

1. Users shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied

access to the network.

- B. Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed by all users to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

IX. COPYRIGHT/SOFTWARE

- A. The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.

X. CONSEQUENCES FOR INAPPROPRIATE USE

- A. The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.
- B. Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services may be reported to the appropriate legal authorities for possible prosecution.
- C. Loss of access to computer resources and other disciplinary actions up to and including suspension or expulsion from school shall be consequences for inappropriate use.
- D. Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.
- E. Violation of this Policy may result in disciplinary action pursuant to due process procedures established by Board Policy, state and federal law, and/or collective bargaining agreements.

XI. SAFETY

- A. To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who received threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.
- B. Any School computer/server utilized by students and staff shall be equipped with a technology protection measure that blocks or filters Internet access to materials that are obscene, child pornographic, or

harmful to minors (as though terms are defined by CIPA).

C. Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "Hacking" and other unlawful activities.
4. Unauthorized disclosure, use and dissemination of personal information regarding minors.
5. Restriction of minor's access to materials harmful to them.

D. The technology protection measure may be disabled by a California Area School District staff member for "bonafide" research purposes to be undertaken by an adult, provided the adult is not a secondary student.

E. A California Area School District staff member may override the technology protection measure for a student to access a site with legitimate educational value that is blocked by the technology protection measure, provided access is not given to any obscene, child pornographic or other material harmful to minors.

XII. USER AGREEMENTS

A. The Superintendent and/or designees shall develop user agreements to be executed by students, parents and staff, pursuant to this policy.

EMPLOYEE INTERNET USE ACKNOWLEDGEMENT FORM

I, _____ an employee of the California Area School District, hereby acknowledge that I have read and am familiar with the Responsible Use Guidelines established by the School District for an employee's use of the Internet at the School District, and agree to comply with said Responsible Use Guidelines. I recognize and agree that the executed original of this Acknowledgement Form shall be maintained in my personnel file within the California Area School District.

Date: _____

Signature: _____

Printed Name: _____