

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
PLEASANTON ISD STUDENT & EMPLOYEE ACCEPTABLE USE POLICY

CQ
REGULATION

[5/13/2008]

Dear Employee:

Pleasanton Independent School District has an Employee and Student Acceptable Use Policy to be in compliance with the (CIPA) Children's Internet Protection Act (HR4577). Pleasanton ISD has used filtering software since Internet usage was introduced in our schools.

It is necessary for you to read and review the policy and sign the Employee Agreement Form. If you have questions, feel free to contact your supervisor.

Sincerely,

Bernard Zarosky
Superintendent

Pleasanton ISD

Employee Acceptable Use Policy

Proposed for Adoption by PISD Board: 5/13/2008

Acceptable Use Policy updated May 13, 2008



The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

USE BY MEMBERS OF THE PUBLIC

Access to the District's electronic communications system, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use may be permitted so long as the use:

1. Imposes no measurable cost on the District; and
2. Does not unduly burden the District's computer or network resources.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Non-compliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH (Employee Standards of Conduct), FN series (Student Rights and Responsibilities), FO series (Student Discipline), and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act (CIPA) and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices and may disable the technology protection measure to enable access to bona fide research or for another lawful purpose for adults.

MONITORED USE

Electronic mail transmissions and other use of the electronic communications system by students and employees *shall not be considered private*. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet. The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in the proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

CONSENT REQUIREMENTS

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work.

No personally identifiable information about a District student will be posted on any Web page under the District's control unless the District has received written consent from the student's parent. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy.

FILTERING

The Superintendent will appoint a committee, to be chaired by the Technology Director, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

SYSTEM ACCESS

Access to the District's electronic communications system will be governed as follows:

1. Students in grades PK-12 will be granted access to the District's system by parental permission, as appropriate. Students in grades 5-12 may be assigned individual accounts. District employees should make every effort to monitor that student user accounts are being used in accordance with the Student AUP.
2. District employees will be granted access to the District's system upon receipt of the signed Employee Acceptable Use Policy.
3. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.
4. All users will be required to sign a user agreement annually for issuance or renewal of an account.
5. With parental permission, students will be granted access to the system and the District Internet Access pass must be prominently displayed on top of the monitor (on campuses that require it), for every student using or viewing the Internet.

RESTRICTIONS

1. Installing any programs to the District's network system is prohibited.
2. Copying and distribution of unauthorized materials such as but not limited to video, audio, and image files is prohibited.
3. Use of district equipment for personal financial gain is strictly prohibited.
4. Accessing the district network using any non-district devices is prohibited.(example – a personal wireless laptop)
5. Damaging and vandalizing computers, computer systems or computer networks is prohibited.
6. Printing non-course related materials is strictly prohibited.
7. Accessing and using non-district provided email is strictly prohibited.

TECHNOLOGY COORDINATOR RESPONSIBILITIES

The Technology Director for the District's electronic communications system will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign annually an agreement to abide by the District policies and administrative regulations regarding such use. All such agreements will be maintained on file as designated by the principal or supervisor.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
PLEASANTON ISD STUDENT & EMPLOYEE ACCEPTABLE USE POLICY

CQ
REGULATION

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system.
6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed inappropriate.
7. Set limits for data storage within the District's system, as needed.

INDIVIDUAL USER RESPONSIBILITIES
ON-LINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use. Users are expected to make every effort to keep their passwords private and confidential; sharing passwords is prohibited and will result in disciplinary action. Users are required to change their passwords periodically to maintain confidentiality.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.
3. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.
4. Communications may not be encrypted so as to avoid security review by system administrators.
5. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.
6. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.
7. Students should never make appointments to meet people whom they meet on-line and should report to a teacher or administrator if they receive any request for such a meeting.
8. System users must purge electronic mail in accordance with established retention guidelines.
9. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
PLEASANTON ISD STUDENT & EMPLOYEE ACCEPTABLE USE POLICY

CQ
REGULATION

10. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.
11. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
12. System users should be mindful that use of school-related electronic mail address might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.
13. System users may not waste District resources related to the electronic communications system.
14. System users may not gain unauthorized access to resources or information.
15. System users may not attempt to bypass filtering devices or security software with the use of proxies or other means to gain access to restricted or district-blocked Internet sites. To do so is a violation of the Acceptable Use Policy and may result in suspension or revocation of system access and may also be punishable according to campus policies.
16. All, but not limited to, external media storage devices such as floppy disks, flash/jump drives, CD-R/RW, and storage cards must be scanned by a staff/faculty member for viruses.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

INFORMATION CONTENT/THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

PARTICIPATION IN CHAT ROOMS *(AND NEWSGROUPS)*

No participation in any chat room *(or newsgroup)* accessed on the Internet is permissible for students or employees.

DISTRICT WEB SITE

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Webmaster. The Technology Director and the District Webmaster will establish guidelines for the development and format of Web pages controlled by the District.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent.

No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL OR CLASS WEB PAGES

Schools or classes may publish and link to the District's site Web pages that present information about the school or class activities, subject to approval from the Webmaster. The campus

principal will designate the staff member responsible for managing the campus ' s Web page under the supervision of the District ' s Webmaster. Teachers will be responsible for compliance with District rules in maintaining their class Web pages. Any links from a school or class Web page to sites outside the District ' s computer system must receive approval from the District Webmaster.

STUDENT WEB PAGES

With the approval of the District Technology Director, students may establish individual Web pages linked to a campus or District Web site; however, all material presented on a student ' s Web page must be related to the student ' s educational activities. Student Web pages must include the following notice: "This is a student Web page. Opinions expressed on this page shall not be attributed to the District." Any links from a student ' s Web page to sites outside the District ' s computer system must receive approval from the District Webmaster.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the District Webmaster, extracurricular organizations may establish Web pages linked to a campus or District Web site; however, all material presented on the Web page must relate specifically to organizational activities and include only student-produced material. The sponsor of the organization will be responsible for compliance with District rules for maintaining the Web page. Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District." Any links from the Web page of an extracurricular organization to sites outside of the District ' s computer system must receive approval from the District Webmaster.

PERSONAL WEB PAGES

District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude. Use upper and lower case letters as appropriate to letter writing or business communication.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited. System users are strongly encouraged to use their e-mail addresses only for education-related communication.

TERMINATION/REVOCAION OF SYSTEM USER ACCOUNT

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
PLEASANTON ISD STUDENT & EMPLOYEE ACCEPTABLE USE POLICY

CQ
REGULATION

will meet the system user ' s requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Pleasanton ISD

Email Login Signup & Procedures

We have an email server that enables PISD email clients to send/receive email via the World Wide Web anywhere in the world. All teachers have Internet access in their classroom.

Teachers, all we need for you to do is:

1. Fill out the form below.
2. Read the attached **Acceptable Use Policy** and sign and return the Employment Agreement For An Electronic Communications System Account form.
3. **Send this form back to your principal in a sealed envelope**, for security reasons. It is important that you return this form to your principal by _____. **On the outside of the envelope, please put the word "Tech Dept./Email"**.
4. You will be notified via your voicemail when your account has been activated. We will also be providing campus-based email training as needed for new teachers on different campuses, so watch for it.

First Name: _____ Middle Initial: _____ Last Name: _____

Campus: _____ Department: _____

Grade#: _____ Voice Mail#: _____

Desired Email Password: _____
(Please no capitalization or spaces, letters and numbers only, 4-10 characters)

Your Signature: _____

The email address should be your first initial, middle initial, and your last name. In some cases this may conflict with another user's address, so we may have to use your full first name. Your address will be your username@pisd.us. For example: mnate@pisd.us is Maria Naté's email address.

THERE IS MORE TO FILL OUT ON THE BACK OF THIS PAGE

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(Exhibit)

EMPLOYEE AGREEMENT FOR AN ELECTRONIC COMMUNICATIONS SYSTEM ACCOUNT

I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. In consideration of the privileges of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including without limitation, the type of damages identified in the District's policy and administrative regulations

Signature: _____ Date: _____

Printed Name: _____ Campus: _____

Home address: _____

Home phone number: _____ Campus Phone Ext: _____

This space reserved for PISD Administrative offices:

Employee identification verified and account approved for creation by:

Personnel Office: _____ Date: _____

Central Office: _____ Date: _____

This space reserved for Network Administrator:

Assigned username _____

Assigned password _____

Account creation date _____

Account created by _____

***To be returned to your principal
no later than _____.***