Acceptable Use Policy
AUP

Canutillo Independent School District
Canutillo, Texas

Mailing Address:
P.O. Box 100
Canutillo, TX 79835

Located at:
7965 Artcraft Road
El Paso, Texas 79932

(915) 877-7400

Revised: July 2009

Non-Discrimination Statement

Public Notification of Nondiscrimination

Canutillo Independent School District does not discriminate on the basis of race, religion, color, national origin, gender, age, disability or military status in its employment practices or in providing education services, activities, and programs, including vocational programs, in accordance with Title VI and Title VII of the Civil Rights Act of 1964, as amended; Title IX of the Educational Amendments of 1972; and Section 504 of the Rehabilitation Act of 1973, as amended.

For information about rights or grievance procedures, contact the Title IX Coordinator, Renee O'Donnell, (915) 877-7401 and/or the Office - 7965 Artcraft Road, El Paso, Texas 79932 Mail - P.O. Box 100, Canutillo, Texas 79835

Canutillo Independent School District (ISD) Telecommunications Network (CanutilloNet) Application for Account and Terms and Conditions for Use

Overview

The Canutillo ISD Network (CanutilloNet) makes electronic network services available for the students, staff, and community members of Canutillo, Texas. Our goal in providing CanutilloNet is to promote educational excellence in the Canutillo Schools and facilitate resource sharing, innovation, and communication. The CanutilloNet includes: Distance Education, video conferencing, library systems, campus systems, administrative systems, telephone systems, wireless communication, or any other electronic telecommunication system.

The Internet is an electronic highway connecting thousands of computers all over the world to millions of individual subscribers who have access to electronic mail, information and news from research institutions, colleges and libraries, and discussion groups on a wide variety of topics. Also, with access to computers and people all over the world comes the availability of material that may not be acceptable in and educational environment. In a global environment, it is impossible to control all materials, and an industrious user may discover controversial information.

Internet access is coordinated through a complex association of governmental, district, regional, and state networks. In addition, the smooth operation of the District's systems and networks rely upon the proper conduct of the end users who must adhere to the school district's guidelines. In general, this requires efficient, ethical, and legal utilization of the school district's network.

If a CanutilloNet user violates any provisions of the AUP, his or her account will be terminated and future or limited access could possibly be denied. Acceptance of Canutillo's AUP is legally binding and indicates the party (parties) who have read the terms and conditions carefully and understand(s) their significance.

The Superintendent or designee will oversee the District's electronic communications system. The District will provide training in 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. Designee is the Executive Director of School Resources.

RULES OF APPROPRIATE SYSTEM USE

1. All system accounts are to be mainly used for identified education purposes, but some limited personal use is permitted.
2. All system users (employee, students, and non-school user) will be held responsible at all times for the proper use of their account, and the District may suspend or revoke their access if the rules are violated.
3. Remember that people who receive e-mail from a district user (employee, students, and non-school user) with a school address might think your message represents the school's point of view.

VIOLATION OF ACCEPTABLE USE POLICY

Depending upon the type and severity of the offense, the district may enact the following consequences, but the District and the Superintendent's Designee reserves the right to alter these consequences on an as needed basis and without prior notification. [See CQ(EXHIBIT on Staff Consequences for Inappropriate Use of AUP violation, Student Consequences for Inappropriate Use of AUP, and Non-School User Consequences for Inappropriate Use of AUP)]

INTERNET/CYBER SAFETY

Willful and repeated misuse of cell phones, computers, and other electronic communication devices to harass and threaten others is a considered a form of cyber-bullying. This includes instant messaging, chat rooms, e-mails, and messages posted on websites. [See FFI(Local) Student Welfare Freedom from Bullying and the district's student code of conduct]

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 using electronic communications.
3. Prevent unauthorized access, including hacking and other unlawful activities.
4. Restrict unauthorized disclosure, use and dissemination of personally identifiable information regarding students.
5. Educate students about cyber-bullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms.

CONSENT REQUIREMENTS

1. 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.
2. 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. In the case of a system design, the individual involved will be asked to sign an "Intellectual Property Rights" document.
3. All Canutillo Websites are copyrighted.
4. No personally identifiable information about a District student will be posted on a 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. [See CQ(EXHIBIT) and policies at FL]

FILTERING

The Superintendent will appoint a committee, to be chaired by the Executive Director of School Resources, 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, gang related activities, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

REQUESTS TO DISABLE FILTER

Requests from users who wish to use a blocked site for bona fide research or other lawful purposes are to submit a written request to their Campus Administrator for initial approval and then to the district's Information Technology Department. Requests will be reviewed on a case by case basis.

SYSTEM ACCESS

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

1. Students in grades **pre K through 12** will be assigned individual accounts upon completion of an AUP form with parental approval.

2. Students are prohibited from participating in any chat room (or newsgroup) accessed on the Internet. Such participation is permissible for employees, under special conditions. Chat room participation in an educationally approved portal must be approved by Campus Administrator and the Executive Director of School Resources.
3. District employees will be granted access to the District's system upon completion of an AUP form.
4. The District will require that all passwords be changed every 360 days or less.
5. 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.
6. All users will be required to sign a user agreement annually or as required for issuance or renewal of an account.

EXECUTIVE DIRECTOR OF SCHOOL RESOURCES RESPONSIBILITIES

The Executive Director of School Resources 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 annually (or as required) complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained in a file in the principal's office or an online log file.
3. Ensure that employees supervising students who use the District's system provide training in the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student and staff safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose.
7. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
8. Set limits for data storage within the District's system.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

ON-LINE CONDUCT

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
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 by users 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 Executive Director of School Resources, as appropriate.

6. System users, especially 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. System users, especially 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 daily or as appropriate.

9. System users may not redistribute copyrighted programs, music, 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 in a written format from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations. A copy of the copyright release must be sent to the Information Technology Department prior to the distribution of the copyright document or data.

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 upload or download public domain programs to the system without prior approval.

12. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

13. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

14. System users should be mindful that use of school-related electronic mail addresses 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.

15. System users may not waste District resources related to the electronic communications system. Some examples may include, but not limited to: electronic chain letters, massive e-mailings of jokes, massive emailing to join a lottery, personal agendas that may be political or religious in nature. The use of network resources must be in line with the district’s educational mission.

16. Gaining unauthorized access to restricted information or resources.
17. Use of proxies to bypass filtering and security is prohibited.
18. Access either by direct URL or proxy URL to social networks such as MYSpace, Facebook or other is prohibited.
19. Misuse of command line language as a CHAT venue is prohibited.
20. Attempting to plug in unauthorized (personal) equipment such as computers or laptops to CISD network is prohibited.
21. Any attempt to bypass network security/filters is prohibited.
22. Sharing of your user profile (sign-on and password) may lead to disciplinary action up to and including termination.

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 or massive emailing.
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.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action including termination in accordance with District policies. [See DH]

PARTICIPATION IN CHAT ROOMS (AND NEWSGROUPS)

Students are prohibited from participating in any chat room (or newsgroup) accessed on the Internet. Such participation is permissible for employees, under special conditions. Chat room participation in educationally approved portal must be approved by Campus Administrator and the Executive Director of School Resources.

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 Executive Director of School Resources or designee will establish guidelines for the development and format of Web pages controlled by the District.

1. 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 or guardian.
2. No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL, CLASS, or DEPARTMENT WEB PAGES

Schools, classes, departments, divisions may publish and link to the District's site Web pages subject to approval from the Executive Director of School Resources or designee. The Campus Principal, Department Director, or Executive Director will designate a staff member responsible for managing the campus's, department's, or divisions Web page under the supervision of the Executive Director of School Resources or designee. Teachers will be responsible for compliance with District rules in maintaining their class Web pages and any links. Web page links to sites outside the District's computer system must receive approval from the Executive Director of School Resources or designee.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the Executive Director of School Resources or designee, 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 organization 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 the District's computer system must receive approval from the Executive Director of School Resources or designee.

PERSONAL WEB PAGES	District employees, Trustees, and members of the public will not be permitted to publish personal Web pages using District resources.
STUDENT WEB PAGES	The District will not permit Web pages maintained by students, linked to the District Web site.
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. 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. (e.g., massive emailing)
TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT	Termination of access to the district's computer network for violation of AUP policies or regulations will be effective on the date the Campus Administrator, Executive Director of Human Resources, or Executive Director of School Resources receives notice of student, staff, or community member's withdrawal or of revocation of system privileges, or on a future date if so specified in the written notice.
DISCLAIMER	The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express 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 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.
COMPLAINTS REGARDING	The District designates the following employee to receive any complaints that copyrighted material is improperly contained in the

COPYRIGHT COMPLIANCE

District network:
Name: LuAnn Escobar
Position: Executive Director of School Resources
Address: P.O. Box 100 Canutillo, Texas 79835
Telephone: 915.877.7460
E-mail: lescobar@canutillo-isd.org

COMPUTER EQUIPMENT LIABILITY

Employees and students are responsible for the condition of all school property (textbooks, library books, and electronic devices) checked-out to them. A charge may be assessed if school property is lost or damaged beyond normal wear.

Any employee who willfully damages school property, or fails to return property lent to him/her when it is requested, will be liable for repair or replacement of damaged and/or unreturned items, and shall subject himself/herself to disciplinary action.

Any child who willfully damages school property, or fails to return property lent to him/her when it is requested, shall cause his/her parents to be liable for repair or replacement of damaged and/or unreturned items, and shall subject himself/herself to disciplinary action.

TRANSFER OF EQUIPMENT TO STUDENTS

The following rules will apply to all campuses, departments, and divisions regarding transfer of computer equipment to students under provisions of law cited at CQ(LEGAL):

1. Proposed projects to distribute computer equipment to students must be initiated by completing an *Asset Checkout Request Form* and submitting the form to the Executive Director of Business Services.
2. A student is eligible to receive computer equipment under these rules only if the student does not otherwise have home access to computer equipment, as determined by the Campus Administrator and counselor.
3. In transferring computer equipment to students, the Campus Administrator will give preference to educationally disadvantaged students.
4. Before transferring computer equipment to a student, the Campus Administrator or designee must have an **approved** *Asset Checkout Request Form* and have clearly outlined:
   a. A process to determine eligibility of students;
   b. Has clearly informed the student/parent of the responsibility and liability regarding home placement, use, and ownership of the equipment;
   c. A process to distribute and initially train students in the setup and care of the equipment;
   d. A process to provide ongoing technical assistance for students using the equipment;
   e. A process to determine ongoing student use of the equipment;
   f. A process to determine any impact on student achievement the use of this equipment may provide;
   g. A process for retrieval of the equipment from a student, as

necessary; and

h. If a loss or damage occurs a *Notification of Missing/Stolen Property Form* and a police report must be filed within 5 working days. In the event of loss, the Capital and Controlled Asset Management - Missing and Stolen Property procedure must be followed in the submittal of forms. In addition, copies of this report will be forwarded to the IT Department within 10 working days of filed report by the Business Services Accountant. Assessment of reimbursement will be based on a prorated basis to be determined by the Executive Director of School Resources.

TRANSFER OF EQUIPMENT TO STAFF MEMBERS

The following rules will apply to all campuses, departments, and divisions regarding transfer of computer equipment to staff members under provisions of law cited at CQ(LEGAL):

1. Proposed projects to distribute computer equipment to staff members must be submitted to the Executive Director of Business Services for initial approval via an *Asset Checkout Request Form*.
2. Before transferring computer equipment to a staff member, the Campus Administrator or Administrator must have an **approved** *Asset Checkout Request Form* and have clearly outlined:

a. Has clearly informed the staff member of the responsibility and liability regarding home placement, use, and ownership of the equipment;

b. A process to distribute and initially train the staff member in the setup and care of the equipment;

c. A process to provide ongoing technical assistance for the staff member using the equipment;

d. A process to determine ongoing staff member's use of the equipment;

e. A process for retrieval of the equipment from the staff member, as necessary; and

f. If a loss or damage occurs a *Notification of Missing/Stolen Property Form* and a police report must be filed within 5 working days. In the event of loss, the Capital and Controlled Asset Management - Missing and Stolen Property procedure must be followed in the submittal of forms. In addition, copies of this report will be forwarded to the IT Department within 10 working days of filed report by the Business Services Accountant. Assessment of reimbursement will be based on a prorated basis to be determined by the Executive Director of School Resources.