

Refugio Independent School District

Acceptable Use Policy for Refugio ISD Students

— OVERVIEW —

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Refugio ISD provides Internet access and computer resources to its students, teachers, and administrators to promote educational excellence in Refugio ISD by facilitating resource sharing, innovation, and communication.

The District's computer resources are intended to assist in the collaboration and exchange of information between and among schools, district offices, educational service centers, the Texas Education Agency, and other State and Federal educational entities. To achieve our goal of promoting innovation and educational excellence, the computer resources are intended to provide quality, equitable, and cost-effective information and communication resources to the educational community.

With this educational opportunity also comes responsibility. The smooth operation of the computer network requires user compliance with the acceptable use guidelines reflected in this Acceptable Use Policy (AUP). If a user violates any of these provisions, his or her account may be terminated and future access to the computer system could be denied, and the student could be disciplined in accordance with the Student Code of Conduct.

— CONTENT —

The Internet is an association of diverse communication and information networks. While the District is required by federal law to use technology protection measures to limit access to material considered harmful or inappropriate to students, it may not be possible for the District to absolutely prevent such access. Despite our best efforts and beyond the limits of filtering technology, students and parents should be aware that use of the system may provide access to other systems in the global network that contain inaccurate, objectionable, or adult material. A student that gains access to such material must discontinue access as quickly as possible and must report the incident to the supervising teacher, administrator, or technology coordinator.

— SYSTEM ACCESS —

Access to the District's computer resources is a privilege, and not a right. Student users violating the computer resource guidelines contained in this AUP are subject to suspension of system access, revocation of the computer system account, or other discipline in accordance with the Student Code of Conduct. All student users will be required to sign the AUP annually in order to receive access to the District's computer resources.

Students will be granted access to the District's computer resources by the technology coordinator or supervising teacher, as appropriate. No student will be assigned an individual account or password for Internet or email use. However, students may be assigned passwords on a limited basis for classroom use related to the completion of class work. This access will be given with the written approval of the immediate supervisor and with a request from the teacher for a class account.

- Electronic mail transmissions and other use of the District's computer resources are not private and may be monitored to ensure appropriate use at any time by Internet service providers, operators of system file servers, and designated District staff.
- Any system user identified as a security risk or as having violated the AUP may be denied access to the District's system and may be disciplined in accordance with the Student Code of Conduct.
- Users should promptly report violations of the AUP to the supervising teacher, administrator, or the technology coordinator.

— USER RESPONSIBILITIES —

The following standards apply to all student users of the district's computer resources:

- Students are responsible for the proper use of the computer resources for the duration of the student's use.
- The system may not be used for illegal purposes or in support of illegal activities or for any other activity prohibited by District policy, rules, or regulations, or Student of Code of Conduct.
- Participation in any chat room or newsgroup accessed on the Internet is not permitted. Moreover, users may not identify or discuss a student on any system website.
- Users may not disable or attempt to disable a filtering device on the District's electronic communication system.
- Students may not use the District's computer resources, including electronic mail, to distribute personal information about themselves or others. Personal information includes, but is not limited to, address, telephone number, or photographs.
- Students may not use the District's computer resources to make appointments to meet people whom they meet through the Internet. Students should report a request for a meeting to teacher, administrator, or technology coordinator.

- Users may not access or use another person's account or allow anyone else to use their account.
- Users may not (and may not attempt to) read, delete, copy, or modify the electronic mail of other system users.
- Users may not deliberately interfere with the ability of other system users to send and/or receive electronic mail.
- Users must purge electronic mail in accordance with the established retention guidelines.
- No user may 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. Copyright protections may apply to music, videos, or other items located on the Internet. The contents of the Refugio ISD web page are copyrighted; and no, text, image, or other materials on it may be copied, retransmitted, redisplayed, or modified without the District's express written consent.
- Users should avoid actions that increase the risk of introducing viruses to the system, such as opening email messages from unknown senders and loading data from unprotected disks or computers.
- Users may not make deliberate attempts to disrupt or degrade system performance including, but not limited to, uploading or creating computer viruses.
- Users may not upload or download public domain programs to the system without the direct permission of the teacher or technology coordinator. Users are responsible for determining whether a program is in the public domain.
- Users may not send/post messages/images or purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing damaging to another's reputation, illegal, or otherwise in violation of any provision of District policy or this AUP.
- Users may not send non-school related mass messages.
- Use of the District's resources, including electronic mail, for product advertisement, profit making pitches, or political lobbying is not permitted.
- Users may not pretend to be someone else when sending or receiving messages. Likewise, forging communications or posting anonymous messages is prohibited.
- Users may not encrypt their communications so as to avoid security review.

If you would like a hard copy of this policy, please contact the campus: RES 526-2364; RJHS 526-2434; RHS 526-2344

- Use appropriate language; profanity, obscenity, and ethnic/racial slurs are prohibited.
- Be mindful that use of school-related electronic mail addresses might cause recipients or other readers of that mail to assume the user (and the message in the electronic mail) represents the District, whether or not that was the user's intention.
- Using a school-related electronic mail address in a manner contradictory to District policies or regulations is prohibited.
- Users may not gain unauthorized access, including hacking, to resources or information.
- Users may not use the network in such a way that would disrupt the use by others.
- The system may not be used for financial or commercial gain or business use.
- Use for commercial activities by for profit institutions is not permitted.
- Users may not knowingly access or bring prohibited materials into the electronic environment.
- Users should report to the teacher, administrator, or the technology director when they receive or encounter information on the District's computer resources that they think is inappropriate.
- Users may not attempt to harm or destroy District equipment or data or the data of another or of any of the agencies or other networks connected to the Internet.
- Teachers are responsible for supervising student computer use in their classroom.

— CYBER BULLYING —

Refugio ISD strives to provide a safe, positive learning climate for students and staff in the schools. Therefore, users will maintain an educational environment in which bullying and cyber bullying in any form are not tolerated.

All forms of bullying and cyber bullying by school district staff and students are hereby prohibited. Anyone who engages in bullying or cyber bullying shall be subject to appropriate discipline.

Definitions:

Bullying shall mean unwelcome verbal, written or physical conduct directed at a student or staff member by another student or staff member that has the effect of:

1. Physically, emotionally or mentally harming a student;
2. Damaging, extorting or taking a student's personal property;
3. Placing a student in reasonable fear of physical, emotional or mental harm;
4. Placing a student in reasonable fear of damage to or loss of personal property; or
5. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

Cyber bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, digital pictures or images, or website postings (including blogs) which has the effect of:

1. Physically, emotionally or mentally harming a student or staff member;
2. Placing a student or staff member in reasonable fear of physical, emotional or mental harm;
3. Placing a student or staff member in reasonable fear of damage to or loss of personal property; or
4. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

Delegation of Responsibility:

Each student and staff member shall be responsible to maintain an educational environment free of bullying and cyber bullying.

Each staff member and student shall be responsible to respect the rights of his/her fellow staff members and all students and to ensure an atmosphere free from all forms of bullying and cyber bullying.

Students shall be encouraged to report bullying or cyber bullying complaints to any staff member. Any staff member who receives a bullying or cyber bullying complaint shall gather information or seek administrative assistance to determine if bullying or cyber bullying has occurred.

If you would like a hard copy of this policy, please contact the campus: RES 526-2364; RJHS 526-2434; RHS 526-2344

— SOCIAL NETWORKS —

Definition

A social network is a service that uses the Internet for online communication through an interactive network of photos, web logs, user profiles, e-mail, web forums, and groups, as well as other media.

- * Social networking sites gather data submitted by members as "profiles"
- * Profiles can then be shared among members
- * Membership can be free or fee-based

Be safe

Anyone can access the Internet and view what you write on a social network site. Even if your page is 'protected' there is nothing to stop your friends from copying your material and placing it elsewhere on the web. It is important to respect your privacy. Use your first name only and do not use pictures of yourself. If you wish to have an image associated with your blog, use a picture of something that represents you. Don't give out any personal information about yourself or anyone else.

Do not search for illegal, crude, rude, crass and inappropriate things.

Do not harass other students through blogs.

Do not copyright infringe or plagiarize or download anything illegally.

— 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 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 the 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 computer resources.

STUDENT ACCEPTABLE USE POLICY FOR COMPUTER RESOURCES

Student's Printed Name

I have read this Acceptable Use Policy and the District's CQ (regulation); I agree to abide by the provisions contained in those documents.

I understand that my failure to comply with the provisions of the Acceptable Use Policy or CQ (regulation) may result in suspension of system access, revocation of the computer system account, or discipline in accordance with the Student Code of Conduct.

I understand that it is impossible for Refugio ISD to restrict access to all controversial materials that may be found on electronic networks, and I will not hold the District responsible for material I encounter while using District computer resources.

Electronic mail transmissions and other use of the District's computer resources are not private and may be monitored to ensure appropriate use at any time by Internet service providers, operators of system file servers, and designated District staff.

I will report any misuse of the information system as identified in the Acceptable Use Policy or CQ (regulation) to the Refugio ISD technology coordinator, teacher, or an appropriate campus administrator.

In consideration for the privilege of using the District's computer resources 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.

Student Signature

Date

Parent Signature

Date