

Acceptable Use Policy

Santa Rosa Independent School District
232 East Jesus T. Avila Avenue, Santa Rosa, Texas 78593

GUIDELINES

Operation of the Internet relies heavily on the proper conduct of the users, who must adhere to strict guidelines. To remain eligible as users, its use must be in support of and consistent with the educational objectives of the school district. Access is a privilege, not a right. Access entails responsibility. If a user violates any of the acceptable use provisions outlined in this document, future access will be denied. Any user violating the provisions contained herein, any applicable state or federal law, policies posted in classrooms, and/or district policies in effect will be subject to the loss of Internet access privileges. District disciplinary action consistent with district policies will be taken accordingly.

Acceptable Use means that the information must be:

- in support of education and research consistent with district policy
- consistent with the rules appropriate to any network being used/accessed and generally accepted rules of network etiquette.

  It is advisable to notify the Information Technology Department immediately if you see any inappropriate web sites or any security problem. Also, inform the Technology Department if there should be changes in your account. (name change, campus change, etc.)

Unacceptable Use means that a user is prohibited from:

- making unauthorized use or downloading of copyrighted information including music and movies
- sending unsolicited bulk mail (UBE or SPAM), transmitting distributing, uploading, posting of any material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful and vulgar
- using the school account for any personal, non-school commercial activities such as advertising or procurement for profit
- using the network for political or lobbying purposes
- using the network or the Internet to induce, solicit, or participate in any unlawful activity such as gambling, extortion, pyramid schemes, chain letters, or the viewing of lewd materials
- disabling or by-passing any installed filtering device (i.e. hacking) or gaining access to any account not belonging to the user (i.e. cracking)
- making available or using any software, program, product or service that is designed to violate this AUP
- gaining access to restricted resources and information
- using devices and applications that put the network at risk**

- identifying or showing security problems to others
- using another person's account
- revealing your account password or allowing another person to use your account
- disseminating your or other's personal identification information

Filtering

In the schools, student access to and use of the electronic mail will be available only through a restricted teacher/staff account. The District-provided Internet access has a filtering device 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 his designee. This filtering device database millions of inappropriate sites and is monitored and updated regularly.

Disclaimer of Liability

The school district makes no warranty of any kind, neither expressed nor implied, for the Internet access it is providing. The District shall not be liable for:

- users' inappropriate use of electronic communication resources or violation of copyright restriction or other laws, users' mistakes or negligence, or costs incurred or unauthorized financial obligation resulting from the District – provided access to the Internet by the user

- ensuring the accuracy, age appropriateness, or usability of any information found on the Internet

- damage to personal property used to access District computers or networks or for District – provided Internet access

- any action of the user who accesses the Internet or any other type of computer networking service from a non-school, business, home, or individual account.

All terms and conditions as stated in this document are applicable to all users of the network. These provisions reflect an agreement of the parties and shall be governed and interpreted in accordance with this policy and the laws of the State of Texas and the United States of America.

Remember

Use of the Internet via the District network is a privilege, not a right. Unacceptable usage may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. Electronic mail transmission and other use of the district's electronic communication are not considered private. Designated district staff is authorized to monitor such communication at any time to ensure appropriate use.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.

For safety-tips visit the following websites:
http://kids.getnetwise.org/safetyguide/
http://www.ftc.gov/kidsprivacy

**Devices and applications that put the network at risk:

- Unauthorized Wireless Access Points (WAPs), personal (non-school) computers or game consoles
- Consumer – grade routers
- Peer-To-Peer applications such as Limewire, BitTorrent, KaZaA, Freenet, eDonkey and Gnutella
- Instant messaging such as Windows Messenger, AOL Instant Messenger and Yahoo!
- Other unauthorized uses of SRISD bandwidth/network resources such as Skype