Red River Parish School District
P.O. Box 1369, 1922 Alonzo Street, Coushatta, LA 71019
(318) 932-4081 FAX (318) 932-3081
www.rrpsb.com

Acceptable Use Policy
for
Red River Parish Computer System and the Internet

RATIONALE

In an effort to provide students and faculty with the vast resources accessible through a computerized information resource system such as the Internet, the Red River Parish School District believes it is necessary for all users to become aware of an acceptable use policy. The benefit of having access to resources from all over the world must be weighed against objectionable materials found on the Internet. In essence we must balance value with liability.

It is the policy of the Red River Parish School District to maintain an environment that promotes ethical and responsible conduct in all online network activities by staff and students. It shall be a violation of this policy for any employee or student to engage in any activity that does not conform to the established purpose and general rules and policies of the network.

All network users will be granted free and equal access to as many network services as their technology hardware allows. Exploration of the Internet is encouraged within the bounds of the Red River Parish mission statement.

The use of the Red River Parish School District's network is a privilege, not a right, and inappropriate use will result in cancellation of that privilege.

ACCOUNTABILITY

Use of school computers or the Red River Parish Computer System (RRPCS) will be reserved for academic or administrative use. All users using a school computer, RRPCS [including the Principal's Administrative Management System (PAMS)] located on school property, or computers accessing the Internet through the RRPCS will be held accountable for their use. This includes, but is not limited to, (a) unauthorized use resulting in expense to the school or school system; (b) equipment damage; (c) use of unauthorized software; (d) privacy and copyrights; (e) tampering; (f) accessing obscene, pornographic, child pornography, any material deemed "harmful to minors", or any materials otherwise inappropriate for educational uses; (g) sending or soliciting inflammatory, abusive, harassing, vulgar, or obscene messages or language; and (h) any action that is deemed inappropriate by the supervisory personnel. Files on the network (RRPCS) will be treated as district property subject to control and inspection, rather than private property which cannot be searched without just cause. Access codes and passwords will be assigned by the RRPCS administrator. The Principal and/or his/her designee will keep records of these accounts in case an inspection is warranted.

UNAUTHORIZED AND ILLEGAL USE

Students must be under the supervision of a teacher, monitor, principal, librarian, or supervisor while using the RRPCS or any school computer. Faculty and staff must be prudent while using the RRPCS or any school computer. Direct supervision for faculty and staff will not be required.

Tampering with selection menus, procedures, or icons for the purpose of misleading or confusing other users is prohibited. Any use of the RRPCS by any person that incurs expenses to the school or school system other than the regular monthly fees and rates is strictly prohibited. Furthermore, the RRPCS will not be used for commercial, political, or religious purposes.

Use of the RRPCS for any hacking or illegal activities is prohibited. Hacking or illegal activity includes but is not limited to (a) tampering with computer hardware and software, (b) unauthorized entry into computers and files, (c) knowledgeable vandalism or destruction of equipment, and (d) deletion of computer files. Such activity is considered a crime under state and federal law.

If an account system is used, users will have full responsibility for the use of their account. All violations of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should an account code or password be given to another user. Impersonations, pseudonyms, and anonymity is not permitted. Real names must be used.

COPYRIGHTS AND PRIVACY

All users must adhere to copyright rules regarding software, authorship, and copying information. The unauthorized copying or transfer of copyrighted materials may result in the loss of network privileges. All software is distributed with a license, which governs its use. Most licenses allow for the copying of the original media (disks or cd-roms) for backup purposes only and for the installation of the software on only one computer. If the software is to be installed on additional computers, additional licenses or original copies of the program must be obtained. If additional licenses or original copies are not obtained, the software must be deleted off the first computer before being installed on a second computer. Users are NOT to bring software from home to school, to install software on school computers without permission, and to violate software copyrights & licenses.

Re-posting personal communications without the original author's prior consent is prohibited. To do this is a violation of the author's privacy. However, all messages posted in a public forum such as newsgroups or listservs (a means of broadcasting an E-mail message for the purpose of maintaining a discussion list) may be copied in subsequent communications, so long as proper credit is given. All E-mail must be deleted as soon as possible after reading in order to conserve file space.

Users are not to access information and files belonging to other staff members, teachers, or students. This includes grades, counseling information, schedules, discipline records, transcripts, test scores, health records, special education records, E-mail, word processing files, and any information protected by law [R.S. 17:1941 and Section 438, PL 93-380].

To protect the online privacy of minors in accordance with the Children's Internet Privacy Act (CIPA), students shall not disclose personal information, such as name, school, address, and telephone number outside of the school network, specifically on the Internet.

INSTALLING PRANK SOFTWARE & VIRUSES

No software is to be added without the permission of the administration.

Avoid the knowing and inadvertent spread of computer viruses. "Computer Viruses" are programs that have been developed as pranks, and can destroy valuable programs and data. To reduce the risk of spreading a computer virus, do not import files or programs from home or from unknown or disreputable sources. If you do obtain software or files from remote sources, follow proper procedures to check for viruses before use. All disks should be scanned for viruses before each use on the RRPCS. State and federal law consider deliberate attempts to degrade or disrupt the RRPCS or the performance of the network or any spreading of computer viruses to be criminal activity.

OBJECTIONABLE MATERIALS

Profanity or obscenity will not be tolerated on the network. All users should use language appropriate for school situations as indicated by school rules and codes of conduct. Avoid offensive or inflammatory speech. The rights of others must be respected both in the local network and the Internet at large. Personal attacks are an unacceptable use of the network. If you are the victim of a "flame", a harsh critical or abusive statement, bring the incident to the attention of an administrator. It is usually better not to respond. Furthermore, retrieving and/or viewing pornographic or obscene materials will not be allowed.

ENFORCEMENT OF POLICY

a. Red River Parish School District uses a technology protection measure that blocks or filters Internet access to block access to some Internet sites that are not in accordance with the policy of Red River Parish School District.
b. The technology protection measure that blocks or filters Internet access may be disabled by a Red River Parish School District staff member for bona fide research purposes by an adult.
c. A Red River Parish School District staff member may override the technology protection measure that blocks or filters Internet access for a student to access a site with legitimate educational value that is wrongly blocked by the technology protection measure that blocks or filters Internet access.
d. Red River Parish School District staff will monitor students' use of the Internet, through either direct supervision, or by monitoring Internet use history, to ensure enforcement of the policy.

Any violation of school policy and rules may result in loss of school-provided access to the Internet. Additional disciplinary action may be determined in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

This policy may be amended by the school district or school to include further restrictions in order to meet special needs, provided that school board policy is not violated.

Approved by Red River Parish School Board on the 4th day of September 2001.