STUDENT INTERNET SAFETY POLICY

SRISD INTERNET SAFETY AND RESPONSIBLE USE POLICY
For STUDENTS

Overview:
The Scurry-Rosser Independent School District provides Internet access to students to promote educational excellence in our schools by facilitating resource sharing, innovation, and communication. If a SRISD user violates any of these provisions, he/she will be subject to loss of privileges on the district s system and will be subject to disciplinary action in accordance with the Student Code of Conduct. This could result in loss of credit for students. A system user is defined as an employee, contracted personnel, or student of SRISD who has access to the computers and/or electronic communication system.

Regulations and Guidelines:
The superintendent or designee will oversee the district's electronic communications system. The district's system will be used only for administrative and educational purposes consistent with the district's mission and goals.

System Access
Access to the district s electronic communications system will be governed as follows:
Upon agreeing to the SRISD's Internet Safety and Responsible Use Policy contained in the student handbook, students will be granted access to the district's system.
Any student user identified as a security risk or having violated district and/or campus computer-use guidelines may be denied access to the district's system. Other consequences may also be taken.

System Conduct

1. All students using the internet and SRISD network 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.
3. System users may not redistribute copyrighted programs or data without 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.
4. Real-time discussions such as chat room and instant messaging are prohibited.
5. Students may not distribute personal information about themselves or others by means of the electronic communication system.
6. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another s reputation, illegal, or violent.

7. System users may not purposefully access or redistribute materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another s reputation, illegal or violent.
8. System users may not waste District resources related to the electronic communication system.
9. System users may not gain unauthorized access to resources or information.
10. All system users are prohibited from playing any type of computer or network game, downloading music, or accessing streaming media not directly related to an approved SRISD curriculum.

Vandalism
Any malicious attempt to harm or destroy district equipment or materials, data of another user of the district s system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of district policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This 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 restitution, hardware, or software costs.

Forgery
Forgery or attempted forgery of electronic mail messages is prohibited. Attempt to read, delete, copy, or modify the electronic mail of other system users to send/receive electronic mail is prohibited.

Information Content/Third Party Supplied
System users and parents of students with access to the district's system should be aware that 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 a suspension and/or a revocation of privileges on the district s system and will be subject to disciplinary action in accordance with the Student Code of Conduct. This could result in loss of credit for students.

Termination of Access
The district may suspend or revoke a system user's access to the district's system upon violation of district policy and/or administrative regulations regarding acceptable use. The termination of a student s access 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.

Consequences of Improper Use
Improper or unethical use may result in disciplinary actions consistent with the existing Student Discipline Policy and, if appropriate, the Texas Penal Code, computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

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 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 the local, state, or federal officials in any investigation concerning or relating to misuse of the district s electronic communication system.