Seminole Independent School District

Acceptable Use Policy
Electronic Communications System

ACCEPTABLE USE MISSION STATEMENT

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and use agreements, consistent with the purposes and missions of the district and with law and policy governing copyright.

AVAILABILITY OF ACCESS

Access to the district's electronic communications system, including the Internet, shall be made available to students and employees for instructional and administrative purposes and in accordance with administrative regulations. Access to the district's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree to comply with such regulations and guidelines. Your login and password (system account) serves as your electronic signature. When logging in you agree to comply with all regulations, guidelines and policies. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary actions consistent with district policies. Violations of law may result in criminal prosecution as well as disciplinary action by the district.

INTERNET USE

The Superintendent or designee shall develop and implement an Internet Safety Plan to:

- Control student's access to inappropriate materials, as well as to materials that are harmful to minors.
- Ensure student safety and security when using electronic communications, which includes but is not limited to email, blogging, podcasts, social networking and messaging.
- Prevent unauthorized access, including hacking and other unlawful activities.
- Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

Each district computer with Internet access shall have a filtering device or software 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 and as determined by the Superintendent or designee. However, no web filtering technology is 100% safe. SISD realizes this fact and takes every effort to monitor online activity. It is your responsibility to report any inappropriate sites that are not blocked by the filter. The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

MONITORED USE

The use of the district's electronic communications system by students and employees shall **not** be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use for educational and administrative purposes. In compliance with federal law and open record requests, SISD must manage electronic data so it can be reproduced in a timely manner. Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

DISTRICT POLICY

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. Commercial use of the district's system is strictly prohibited. The district will provide training to employees in proper use of the system and will provide all users with links to all guidelines and policies. All training in the use of the district's system will emphasize the ethical use of this resource. 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 software purchased and/or approved by the district may be loaded and must be loaded by the district technology director or designee. Only the district technology director or designee may upload copyrighted material to the system.

SYSTEM ACCESS

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

- With the approval of the immediate supervisor, district employees will be granted access to the district's system.
- All system users will be issued a login and password for computer and network services.
- The system user's login and password serves as the user's electronic signature. When logging in the user agrees to comply with all district regulations, guidelines and policies.
- Individuals with system accounts will be required to maintain password confidentiality by not sharing the password with others.
- The individual whose name is associated with the system account will be responsible at all times for its proper use. If your password has been breached it is your responsibility to contact campus designee in order to get it changed.
- System users must use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any inflammatory language is prohibited.
- Revealing personal information including addresses or phone numbers of the user or others is prohibited.
- Any system user identified as a security risk or having violated district and/or campus computer-use guidelines may be restricted or denied access to the district's system.

TERMINATION/REVOCATION OF SYSTEM USER ACCOUNT

The district may suspend or revoke a system user's account upon violation of district policy and/or Student Code of Conduct regarding acceptable use. Termination of a system user's account will be effective on the date the principal or district technology director receives notice of revocation of system privileges, or on a future date if so specified in the notice. Other disciplinary or legal action, in accordance with the district policies and applicable laws may result from inappropriate use.

ILLEGAL ACTIVITIES

Use of the network for any illegal activities is prohibited. Illegal activities include, but are not limited to:

- Tampering with computer hardware or software
- Software piracy
- Unauthorized entry into computers and files (hacking)
- Knowledgeable vandalism or destruction of equipment
- Deletion of computer files belonging to someone other than oneself
- Uploading or creating of computer viruses
- Distribution of obscene or pornographic materials and/or sexting

Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial, legal, and district consequences of such actions are the responsibility of the user (staff, volunteer, and student) and student's parent or guardian.

DISCLAIMER

The district's system is provided on an "as is, as available" basis. The district shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The district shall not be responsible for ensuring the accuracy or usability of any information found on the Internet. The District also will cooperate fully with local, state, and/or federal officials in any investigation related to any illegal activities conducted through the district's communication system.

LINKS

Internet links providing more information and training for Seminole I.S.D. employees and students may be found at http://seminoleisd.net/page/pub.main Information/Technology

AGREEMENT

I have read the district's electronic communications system policy and administrative regulations. I agree to abide by their provisions. In consideration for the privilege of using the district's system and in consideration of 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.