Stephenville Independent School District (SISD) Internet Access Acceptable Use Policy

The purpose of the Stephenville Independent School District provided Internet access is to facilitate communications and expand research/educational opportunities for faculty, administrators, and students. To remain eligible as users, use of the system must be in support of and consistent with the educational mission of SISD. Access is a privilege, not a right. Access entails responsibility.

Any violation of the district's policy and rules relative to Internet or computer use may result in the loss of District-provided access. Additional disciplinary action may be determined at the campus or administrative level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may become involved.

These guidelines and expectations are provided so that SISD employees, students, and guest users are aware of the responsibilities they accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic media, digitalized information resources, communication technologies and Internet access. In general, access requires the efficient, ethical, and legal utilization of all technology resources. Stephenville Independent School District-provided Internet users agree to the following:

Expectations

Use of computers, other technical hardware, computer networks, and software applications are within the scope of the employee's job assignment and/or granted to a student by the student's instructor/administrator.

All users are expected to follow current copyright laws.

All users are expected to notify their immediate supervisor/teacher/administrator of information or messages that are inappropriate, dangerous, threatening, or harassing in nature.

Employees and/or students are expected to use District technology devices within their instructional intent, secure devices when not in use, and/or leave devices in good working condition.

The online presence of employees/students should be in concert with approved Board policies.

Internet/network etiquette

- Be polite
- Avoid use of vulgar or obscene language
- Use caution when giving out addresses or phone numbers (both yours and others)
- Remember, electronic mail is not private or secure
- Do not intentionally disrupt the network or other network users
- Abide by generally accepted rules of network etiquette

Usage guidelines and policies

Commercial use or political lobbying using these electronic resources is prohibited.

Copyrights and others' intellectual property rights are to be observed at all times. Copying of files, software, or passwords belonging to others may constitute theft, plagiarism, or fraud. Software licensed to SISD must be used in accordance with terms of the software license.

Users must always identify him/herself in electronic communications. Anonymous or pseudo-anonymous communications appear to dissociate individuals from responsibility for actions. Concealing user identities or misrepresenting user's names or affiliations to mask or attempt to distance him/herself from irresponsible behavior is a serious abuse of the system. It violates local policies and constitutes fraud.

Follow all security restrictions. Security on any computer system is a high priority, especially when the system involves many users. Do not reveal account passwords or allow others to use any account. Trying to evade, disable, or "crack" a password or other security provision is grounds for immediate suspension of access privileges and other disciplinary action. Users will be held responsible for any misuse of passwords. A user who is identified as a security risk or having a history of problems with other computer systems may be denied access to all SISD Internet services.

Respect the rights of others to freedom from harassment or intimidation. Harassment targets another person or organization to cause distress, embarrassment, injury, unwanted attention, or other substantial discomfort. This includes, but is not limited to, the sending of unwanted mail, chatline comments, postings on social networking sites, and/or any other media resource. Bullying of any nature will not be tolerated.

Use resources efficiently. Please respect the fact that unlimited resources are not available. Time, network bandwidth, printers, paper, disk space, and terminals or PCs are all limited. Restrictions may be placed on any or all of these, as well as any other computing resource. Such restrictions are designed to ensure access for all users.

There is no guarantee of privacy. Electronic communications should not be considered private or secure. In the course of diagnosing, correcting problems, or in response to an official administrative inquiry system administrators may view the contents of any communications or device activity. Individuals' actions or voice may be recorded with or without notice of such.

Obscene communication of any kind, including text or graphic material, is prohibited. This includes any sexually explicit image or other content as specified by local, state, federal, or international laws or policies.

Abide by the policies or guidelines of the network being used. Users are subject to all the rules, regulations or policies of other networks or computer services contacted or connected to from the school or home.

Vandalism is prohibited. Vandalism is defined as any malicious attempt to alter, harm, or destroy data and/or equipment of SISD, another user, the Internet, or other networks. This includes, but is not limited to, creating and/or uploading computer viruses. Possession or use of hacking/keystroke/host-file sharing software is strictly prohibited.

SISD will not be responsible for any damage that users may suffer. This includes loss of data resulting from delays, non-deliveries or service interruptions caused by network failures, computer viruses, or users' errors or omissions. Use of any information obtained via network services is at the users own risk. SISD denies any responsibility for the accuracy or quality of information obtained through network services.

Employees/students are prohibited from using personal computing or related equipment on the District's network without approval from the Director of Technology or his/her designee.

Employees shall refrain from inappropriate communication with a student or minor, including, but not limited to, electronic communication such as a cell phone, text messaging, email, instant messaging, blogging, or other social network communication.

Consequences

The employee/student/guest, in whose name a system account and/or device is issued, will be responsible at all times for its appropriate use.

Non-compliance with the guidelines published here or in related documents outlining accepted District procedures, including but not limited to the Student Code of Conduct, Employee/Student Handbooks, and in Board policies, may result in suspension or termination of technology privileges and/or other disciplinary actions including employment termination. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District.

SISD regards any violation of this policy as a serious offense. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crimes laws. Contents of email and network communications using District equipment and/or network access is governed by the Texas Open Records Act, and when legally requested, proper authorities will be given access to their contents. Cases shall be handled by any of the following: campus principal or his/her campus-level administrative designee and/or Superintendent or his/her district-level administrative designee.

- These individuals/teams with cooperation from the District's Chief Technology Officer shall make final determinations of what is acceptable use.
- SISD Board Policy DGBA (Local), FNG (Legal), and FNG (Local) outline procedures to process appeals or file grievances.

Harassment Complaints

Rules and regulations as outlined in SISD Board Policy DAA, DHB, DHC, FB, FNC shall be enforced in processing harassment complaints filed by users.

Electronic Media and Related

Rules and regulations as outlined in SISD Board Policy GBAA(Legal), DH (Local), BE (Legal), CQ (Local), CPC (Legal), EFE (Local), AIB (Legal), CDA (Local), CFA (Legal), CRD (Legal), DBAA (Legal), DH (Legal), FL (Legal), GBAA (Exhibit). Note that this referenced list of SISD Board Policies includes, but is not limited to those listed and may be expanded or otherwise edited at any time.

I have read the SISD Acceptable Internet Access Acceptable Use Policy and agree to all the terms and conditions.

_____ _____

Print Name Date

_____ _____

Signature Campus/Department