SISD Technology Resources Acceptable Use and Internet Safety Policy

Sabine ISD provides users access to technology resources, including, but not limited to: computers, networks, Google Apps for Education, Video Conferencing, Web applications and other Internet services for **educational purposes only**.

A user (actor) when utilized within this document is defined as:

- Sabine ISD Employee or Board Member
- Sabine ISD Students
- Student Teacher
- Temporary Worker (Substitute Teachers, Consultants, etc.)
- Any third party vendor that uses technology resources in Sabine ISD

Terms and Conditions:

While electronic information resources offer tremendous educational opportunities, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved. The district wants all users to be aware of conduct considered acceptable and unacceptable. Access to Sabine ISD's technology resources will be governed as follows:

- Any system user identified as a security risk or having violated District and/or campus technology use guidelines may be denied access to any SISD technology resource.
- At the beginning of each school year, all users are responsible for reading
Acceptable Use Policy.
- All users must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional guidelines that address software, authorship, and copying information.
- All policies apply to both district technology resources and personal devices.

Instruction:

Each year instruction will be provided to all users regarding appropriate online behavior, including cyber bullying awareness and response, as well as interacting appropriately with other individuals on the Internet. All users will be provided copies of the District's acceptable use guidelines.

It shall be the responsibility of all members of the Sabine ISD staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Monitoring of all District Provided Systems:

- All District technology resources may be monitored whether the use is directly related to school or personal business.
- Monitoring will take place upon the request from the SISD Superintendent or designee.
- The information gathered from the monitoring procedures may be used to provide information regarding appropriate or inappropriate use of the District computer systems and/or required by an authorized legal authority.
- There is no guarantee of privacy, even for "personal" messages.

Internet/Intranet Guidelines, Safety/Filtering, & Social Networks:

Users with access to the Internet through SISD's Network (wired or wireless) will be filtered and blocked from visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by CIPA and as determined by the Superintendent or designee. However, because of the efficiency and ease of creating websites and the increased knowledge and awareness of available methods to bypass Internet filtering systems, it is extremely difficult to completely block every site with objectionable material. The SISD Technology Department, in conjunction with district administrators, campuses, and teachers, continually update the filtering system in an effort to block, to the greatest degree possible, objectionable websites and questionable material.

- Access to SISD's technology resources will be through a District authorized account and for **educational purposes only**.
- Users shall not erase, rename, or make unusable anyone else's computer files, programs or disks.
- Users shall not use, share their own nor attempt to access another user's name, log-on, password, or files for any reason.
- Users shall not use personal devices or SISD computers/networks for any non-instructional or non-administrative purpose (e.g. games or activities for personal profit).
- Users shall not deliberately access or create any obscene or objectionable information, language, or images.
- Users shall not use any social media learning environments (including but not limited to Facebook, blogs, discussion forums, RSS feeds, and message boards) unless they are within a District-approved, safe, secure, curriculum-supported learning activity.

• Users shall not attempt to circumvent the content filtering system through unauthorized means (e.g. proxies, hacking, etc.).
• Streaming media; such as YouTube, Internet Radio, and other online media are for **educational purposes only** and any attempt to circumvent the Content Filter is prohibited.

A user who gains access to objectionable or inaccurate material is expected to discontinue the access as quickly as possible and to report the incident to the appropriate supervisor (teacher, administrator, or district personnel). The site address will be added to filtering software, so that it can be removed from accessibility.

Personal Devices

In some cases, students may find it beneficial or might be encouraged to use personal telecommunications or other personal electronic devices for **educational purposes only** while on campus.
• Students who use personally owned web-enabled devices for educational purposes will have access to a Public wireless network, but will not have access to any district drives such as network folders. Network drives can only be accessed via district equipment. At no time shall a personal device be connected to the SISD wired network.
• SISD is not liable for any loss or damage incurred, nor will it load any software onto student owned devices.
• SISD is not responsible for, nor will SISD reimburse employees or students for any data and/or SMS/MMS (texting) charges.
• All devices should have proper antivirus software and should be clearly marked with the student's name for identification purposes.
• Users will not loan their device to someone else. The user is responsible for the content contained on the device regardless of how it originated. Students are responsible for the security of any equipment brought with them to school.
• Users are not allowed to connect personal printers without the permission of the IT department.
    • If approved, any wireless capabilities must be turned off.
• The IT department will not supply any technical support for personal devices.

All the conditions and requirements of the SISD Acceptable Use Policy are applicable to the use of personal devices. Improper use could result in the loss of privileges for such devices.

Acceptable Use

The District's technology resources must be used for **educational purposes only** and be consistent with the mission and goals of the Sabine Independent School District.

Unacceptable Use

Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities is strictly prohibited. Use for product advertisement or political lobbying is also prohibited.
1. Any malicious attempt to harm or destroy Sabine ISD technology resources, data of another user of the Sabine ISD system, or any of the agencies or other networks that are connected to the Internet is prohibited.
2. A deliberate attempt to hinder or disrupt the system performance may be viewed as a violation 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.
3. Users shall not use a computer for unlawful purposes, such as the illegal copying or installation of software without permission from the holder of the copyright and from the Technology Director. Only designated personnel may install software to any SISD technology resource.
4. Users shall not copy, change or transfer any software or documentation provided by SISD, teachers, or a student without permission from the Technology Director.
5. Users shall not tamper with computers, networks, printers or other associated equipment except as directed by the Technology Department staff.
6. Users shall not connect any personal devices to the SISD wired network. No personal networking equipment, such as Access Points, are permitted on the SISD network.
7. Users shall not move technology equipment (hardware or software) to any other location without written permission from the Technology Director.
8. Messages sent by users may not contain abusive or threatening language, support cyber bullying, must not be sent anonymously or under a false identity and/or contain expressions of bigotry or hate, profanity, obscene comments, or inappropriate materials.

Online Harassment:

Users shall not annoy or harass others with language, images, or threats.

1. An offense under Penal Code Title 7 Chapter 33 Subsection (a) is a felony of the third degree. An offense under Penal Code Title 7 Chapter 33 Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.
2. A person commits an offense if the person uses the name or persona of another person to create a web page or to post one or more messages on a commercial social networking site:
a. without obtaining the other person's consent; and
b. with the intent to harm, defraud, intimidate, or threaten any person.
3. A person commits an offense if the person sends an electronic communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:
a. without obtaining the other person's consent;
b. with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and/or
c. with the intent to harm or defraud any person.
4. If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

If any user disregards the rules set out in SISD's Acceptable Use Policy, the user will be fully liable and Sabine ISD will disassociate itself from the user as far as legally possible.

Consequences of AUP Violation

Violation(s) as defined above will result in:
• suspension of access to the technology resources;
• revocation of the computer system account;
• other disciplinary or legal action in accordance with the District policies and applicable laws.

The Sabine ISD system is provided on an "as is, as available" basis. Sabine ISD does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided, or any information provided, or any software contained on the computer system; the system will meet the 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.
Sabine ISD will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the Sabine ISD electronic communication system.

Disclaimer of Liability:

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, or for costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.