DISCLAIMER OF LIABILITY

The school district makes no warranty of any kind, neither expressed nor implied, for the Internet access it is providing.

The District shall not be liable for:

- Users' inappropriate use of electronic communication resources or violation of copyright restriction or other laws, users' mistakes or negligence, or costs incurred or unauthorized financial obligation resulting from the district-provided access to the Internet by the user.
- Ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.
- Damage to personal property used to access district computers or networks or for district-provided Internet access.
- Any action of the user who accesses the Internet or any other type of computer networking service from a non-school, business, home, or individual account.

All terms and conditions stated in this document are applicable to all users of the network. These provisions reflect an agreement of the parties and shall be governed and interpreted in accordance with this policy and the laws of the State of Texas and the United States of America.

REMEMBER

All users must adhere to the terms in this document. These terms reflect an agreement and are governed by Texas and U.S. laws. All terms and conditions as stated in this document are applicable to all users of the network. These provisions reflect an agreement of the parties and shall be governed and interpreted in accordance with this policy and the laws of the State of Texas and the United States of America.

- Using the Internet through the district network is a privilege, not a right. Misuse can lead to suspension or termination of access and other disciplinary actions. Email and other electronic communications through the district network are not private and may be monitored.
- Families are responsible for guiding Internet use on district devices while off campus.
- Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies, and other possibly offensive media.
- The district will educate students on safe online behavior, including social networking, messaging platforms, and cyberbullying awareness.

For safety tips visit the following websites:

[FTC Protecting Kids Online] (https://consumer.ftc.gov/identity-theft-and-onlinesecurity/protecting-kids-online)

[OnGuard Online] (https://consumer.ftc.gov/identity-theft-and-online-security/onlineprivacy-and-security)

SAN BENITO SCHOOLS

Technology Department
450 S. Dick Dowling St.
San Benito, TX 78586
956-361-6924
fax956-361-6936
www.sbcisd.net

TECHNOLOGY SAN BENITO SCHOOLS

SAN BENITO SCHOOLS

INTERNET ACCEPTABLE USE POLICY

INTERNET ACCEPTABLE USE POLICY

Overview

San Benito Consolidated Independent School District (CISD) iscommitted to fostering educational excellence through the integration of shared resources, innovation, and effective communication. Internet use is an essential component of modern education and should be thoughtfully incorporated into the curriculum. Educators are expected to guide students in the responsible and appropriate use of online resources, treating information from the Internet with the same academic rigor as other instructional materials.

While the District encourages the exploration of digital content, it acknowledges the impossibility of monitoring all information accessible through the global Internet. Accordingly, teachers and staff are responsible for supervising and monitoring students' Internet activity, just as they would with any other classroom instruction.

San Benito CISD employs filtering technologies and implements Internet safety measures in compliance with the Children's Internet Protection Act (CIPA), including FCC Order 11-125, as well as Texas Education Code Chapter 37, Section 37.0832 regarding cyberbullying. Despite these safeguards, complete restriction of inappropriate or noneducational material is not guaranteed. Therefore, users must adhere to all guidelines for acceptable and appropriate use. The District cannot ensure that all content accessed will align with its educational mission, goals, or policies, including CQ (Legal), CQ (Local), and FCC 47 U.S.C. 254, Local FFI.

https://pol.tasb.org/PolicyOnline/PolicyDetails?key=260&code=CQ#localTabContent

https://pol.tasb.org/PolicyOnline/PolicyDetails?key=260&code=FFI#localTabContent

GUIDELINES

Use of the Internet within San Benito CISD is a privilege, not a right. To maintain access, usage must align with the educational objectives and values of the District. All users are expected to act responsibly and in accordance with the policies outlined in this document, as well as applicable classroom rules, District policies, and state and federal laws.

Violations of the acceptable use provisions will result in the loss of Internet access privileges and may lead to further disciplinary action as outlined in District policy. Continued eligibility for access requires ongoing adherence to these responsibilities and standards.

Acceptable Use means:
Users are expected to support educational and research activities that align with district policy and to comply with the rules of any network being accessed, including general standards of network etiquette.

Please notify the Technology Department immediately if you encounter inappropriate websites, detect any security concerns, or experience changes to your account (e.g., name changes, campus reassignment, etc.).

Unacceptable Use means that a user is prohibited from:

- Making unauthorized use or downloading of copyrighted information including music and movies.
- Instant messaging services that are not district-approved.
- Other unauthorized uses of district bandwidth or network.
- Instant messages that are not district approved.
- Other unauthorized uses of district bandwidth or network.
- Devices or Softwares for malicious intent.
- Peer-to-Peer file sharing.
- Accessing resticted resources, devices that put the network at risk.
- Sending unsolicited bulk mail (UBE or SPAM), transmitting, distributing, uploading, posting of any material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful and vulgar (cyber-bulling, sexting).
- Using the school account for any personal, non-school commercial activities such as advertising or procurement for profit.
- Using the network for political or lobbying purposes.
- Using the Network or the Internet to induce, solicit, or participate in any unlawful activity such as gambling, extortion, pyramid schemes, chain letters, or the viewing of lewd materials.
- Disabling or by-passing any installed filtering device (i.e., hacking) or gaining access to any account not belonging to the user (i.e., cracking).
- Making available or using any software, program, product or service that is designed to violate this AUP.
- Gaining access to restricted resources and information.
- Using devices and applications that put the network at risk.**
- Identifying or showing security problems to others.
- Using another person's account.
- Revealing your account password or allowing another person to use your account.
- Disseminating your or other's personal identification information.

** Devices and applications that put the network at risk, but are not limited to:
- Unauthorized Wireless Access Points (WAPs), personal (non-school) computers or game consoles
- Consumer-grade routers
- Peer-to-peer applications such as UmeWire, BitTorrent, Skype, KaZaA, Freenet, eDonkey and Gnutella
- Instant messaging such as Windows Messenger, AOL Instant Messenger and Yahoo!
- Other unauthorized uses of SBCISD bandwidth/network resources such as Skype

Filtering

In the schools, student access to and use of electronic mail will be available through a restricted teacher/staff account. The district-provided Internet access has a filtering device 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 (CIPA) and as determined by the Superintendent or his designee. This filtering device database blocks millions of inappropriate sites and is monitored and updated regularly.
-Staff and student email content is monitored and filtered for inappropriate and/or malicious content.
-Our Internet access includes filtering to block inappropriate content as defined by federal law and district guidelines. This filtering system is regularly updated to block millions of unsuitable sites.