# Acceptable Use of The Computers, Network, Internet, Electronic Communications and Information Systems Policy (AUP)

***Pending Board Approval 7/21/2021***

SANTA ANNA INDEPENDENT SCHOOL DISTRICT

# TABLE OF CONTENTS

# Acceptable Use Of The Computers, Network, Internet, Electronic Communications And Information Systems Policy (AUP)

Santa Anna Independent School District's Acceptable Use of the Computers, Network, Internet, Electronic Communications and Information Systems Policy consists of six sections: Purpose, Definitions, Authority, Responsibility, Delegation of Responsibility, and Guidelines.

## PURPOSE

The Santa Anna Independent School District (SAISD) provides its employees, students, and guests (users) access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, Internet access, mobile devices, peripherals, copiers, and cameras.

The Board supports the use of the district's technology resources to facilitate teaching and learning, to provide access to information, to aid in research and collaboration, to foster the educational mission of the district, and to carry out the legitimate business and operation of the district.

The use of the district's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the district. **Use for educational purposes** is defined as use that is consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the district's technology resources.

All employees and students are responsible for the appropriate and lawful use of the district's technology resources. This policy is intended to ensure that all users continue to enjoy access to the district's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

Users may not use their personal computers to access the School District's Intranet, Internet, or any other CIS system unless approved by the Director of Technology and/or

designee, and/or authorized as part of the School District's services for users.

## AUTHORITY

The Board establishes that access to and use of its technology resources is a privilege, not a right, which may be revoked at any time. The district's technology resources are the property of the district. The district provides these resources for educational and operational purposes as stated herein and are not provided as a public access service or to provide a public forum.

The Superintendent or his/her designee is ultimately responsible for overseeing the district's technology resources. The Superintendent will designate an administrator who will serve as the coordinator and supervisor of the district's technology resources and networks, and who will work with other regional and state organizations as necessary to educate users, approve activities, provide leadership for proper training for all users in the use of the district's technology resources and the requirements of this policy, and who will establish a system to ensure that users who access district technology resources have agreed to abide by the terms of this policy.

The Superintendent or his/her designee is directed to implement Internet safety measures to effectively address the following, both through general policy and through the use of filtering technology on district-provided devices:

1. Access by minors to inappropriate or harmful content.

2. Prevention of unauthorized access of district technology resources.

3. Prevention of unauthorized disclosure and dissemination of minors' personal information.

## DEFINITIONS

**District Technology Resources -** means all technology owned, operated, and/or licensed by the district, including but not limited to computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, routers, and networks, including the Internet.

**User** - means anyone who utilizes or attempts to utilize district technology resources while on or off district property. The term includes, but is not limited to, students, staff, parents/guardians, and any visitors to the district that may use district technology.

## GUIDELINES

### Unauthorized Use Prohibited

Only users who have agreed to abide by the terms of this policy may utilize the district's technology resources. Unauthorized use, utilizing another user's district account, or exceeding one's authorization to use district technology resources is prohibited. Nothing in this policy, however, shall prevent a parent/guardian from assisting his/her child with the use of the district's technology resources, or from monitoring a student's use of the district's technology resources in the student's home as long as it is in adherence to current and future state and federal guidelines including CIPA (Children's Internet Protection Act), COPPA (Children's Online Privacy Protection Act), and FERPA (Family Educational Rights and Privacy Act

### Use of Personal Electronic Devices

The use of personal electronic devices on the district network is permitted only on designated networks. When a user connects a personal electronic device to a district network or district technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a district-owned device were being utilized. Users who connect a personal electronic device to a district network explicitly waive any expectation of privacy in the content exchanged over the district technology resources.

### Privacy

The district reserves the right to monitor any user's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy, and review any and all usage of district technology resources including information transmitted and received via the Internet to ensure compliance with this and other district policies, and state and federal law. All e-mails and messages, as well as any files stored on district technology resources, may be inspected at any time for any reason. The district may

decrypt and inspect encrypted Internet traffic and communications to ensure compliance with this policy.

**Internet Filtering and CIPA Compliance**

The district utilizes content and message filters to prevent users from accessing material through district technology resources that has been determined to be obscene, offensive, pornographic, harmful to minors, or otherwise inconsistent with the district's educational mission. The Superintendent or his/her designee shall establish a procedure for users to request that a legitimate website or educational resource not be blocked by the district's filters for a bona fide educational purpose. Such requests must be either granted or rejected within three (3) school days pursuant to the established procedure.

The Board directs that the Superintendent or his/her designee ensure that students at the elementary, middle school, and high school levels are educated about appropriate online behavior and digital citizenship including interacting via learning management systems and social networks, preventing and reporting cyberbullying, and withholding personal information online.

**Monitoring**

District technology resources shall be periodically monitored to ensure compliance with this and other district policies including monitoring of users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. However, the Superintendent, or his/her designee, shall also implement procedures to ensure that district technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras and/or audio are not utilized except where necessary to recover lost or stolen district technology.

**District-Provided Resources**

District technology resources may be assigned or allocated to an individual user for his/her use (e.g. individual e-mail accounts, laptop computers, etc.). Despite being allocated to a particular user, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of privacy in any district-provided technology resource or any of its contents.

## Cybersecurity

SAISD has implemented network security measures to protect against cyberattack. The users of SAISD resources will not physically connect or attach any unauthorized hardware or equipment to the network. This prohibition includes but is not limited to laptops, cell phones, portable hard drives or other computers designated for "stand alone" operations. However, personal data devices such as listed above may connect wirelessly to the SAISD network. Texas Penal Code section 33.02, Breach of Computer Security, allows for prosecution up to first degree felony for a person who "*...knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.*" SAISD network managers will ensure the maintenance of a content filter, firewall, security settings within the network, password provisions, software and hardware updates, adherence to SFTP protocols, antivirus software, and the education of the end user on practices for cybersecurity safety.

## General Prohibitions

The following uses of district technology resources are prohibited:

1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage others to do so.

2. Use of technology resources to violate any other district policy.

3. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.

4. Use of technology resources to cause, or threaten to cause harm to others or damage to their property.

5. Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate.

6. Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use.

7. Use of technology resources to create, access, or to distribute obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic materials, firearms, or drug

paraphernalia.

8. Use of technology resources to attempt to interfere with or disrupt district technology systems, networks, services, or equipment including, but not limited to, the propagation of computer "viruses" and "worms", Trojan Horse and trapdoor program codes.

9. Altering or attempting to alter other users' or system files, system security software, system or component settings, or the systems themselves, without authorization.

10. The attempted physical harm or attempted destruction of district technology resources.

11. Use of technology resources in a manner that jeopardizes the security of the district's technology resources, or in a manner that attempts to circumvent any system security measures.

12. Use of technology resources to intentionally obtain or modify files, passwords, and/or data belonging to other users or to the district.

13. Use that conceals or attempts to conceal a user's identity, including the use of anonymizers, or the impersonation of another user.

14. Unauthorized access, interference, possession, or distribution of confidential or private information.

15. Using technology resources to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interests.

16. Use of technology resources to commit plagiarism.

17. Installing, loading, or running software programs, applications, or utilities not explicitly authorized by the district technology staff.

18. Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto technology resources.

19. Copying district software without express authorization from a member of the district's technology staff.

20. Use of technology resources for commercial purposes.

21. Use of technology resources for political lobbying or campaigning, not including student elections (e.g. student government, club officers, homecoming queen, etc.).

22. Use of district technology resources to tether or otherwise connect to a non-district owned device to access an unfiltered and/or unmonitored Internet connection.

23. The use of proxies or other means to bypass Internet content filters and monitoring.

24. The use of technology resources to gamble.

25. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.

26. The use of encryption software that has not been previously approved by the district.

27. Sending unsolicited mass e-mail messages, also known as spam.

28. Scanning the district's technology resources for security vulnerabilities.

## DELEGATION OF RESPONSIBILITY

Violations of this policy may result in the temporary or permanent revocation of a user's right to access district technology resources. Additionally, students may be subject to other forms of disciplinary actions for violations of this policy and/or local, state, and/or federal law.

### Limitation of Liability

The Superintendent or his/her designee shall develop procedures, in cooperation with the district technology staff, for the acceptable use of all district technology resources including, but not limited to: software, hardware, electronic devices, servers, and networks.

The district makes no warranties of any kind, whether express or implied, for the service it is providing through its various technology resources. The district is not responsible, and will not be responsible, for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or services interruption. Use of any information obtained through the district's technology resources is at the user's own risk.

**SANTA ANNA INDEPENDENT SCHOOL DISTRICT**
**701 Bowie**
**Santa Anna, TX 76878**

**AUP Acknowledgment and Consent Form**

## Students

I have received, read, and understand this policy and will comply with it. My parent(s)/guardian(s) have reviewed it with me. In addition, I have been given the opportunity to obtain information from the district and my parent(s)/guardian(s) about anything I do not understand, and I have received the information I requested. If I have further questions I will ask my teacher. Additionally, I understand that if I violate the policy, I am subject to the district's discipline and could be subject to ISS, as well as local, state and federal legal recourse.

_____
Name of Student

_____
Signature of Student

_____
Date of Signature

## Parent(s)

As the parent/guardian of a student of the district, I have received, read, and understand the Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy. In addition, I reviewed this policy with my child and answered questions he or she asked. If either my child or I have further questions I will contact the school. I agree to have my child abide by the requirements of the policy.

_____
Name of Parent/Guardian

_____
Signature of Parent/Guardian

_____
Date of Signature

**SANTA ANNA INDEPENDENT SCHOOL DISTRICT**
**701 Bowie**
**Santa Anna, TX 76878**

**AUP Acknowledgment and Consent Form**

## Staff

As an employee of the district, I have received, read, and understand the Acceptable Use of the Computers, Network, Internet, Electronic Communications, and Information Policy. In addition, I reviewed this with my supervisor. If I have further questions, I will contact the administrator for my campus or the Director of Technology. I agree to abide by the requirements of the policy.

_____
Name of Staff Member

_____
Signature of Staff Member

_____
Date of Signature