

ARANSAS PASS INDEPENDENT SCHOOL DISTRICT

ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Please read the following carefully before signing the attached contract.

PURPOSE: Aransas Pass Independent School District (APISD) offers a telecommunications network ("the network") to students, educators and community people for the sole purpose of education. The network is funded by local resources. The school district leverages funds from Universal Services Administration Company-School and Library division (E-rate) and other grant and service providers to assist in the cost. APISD is proud to provide these services and believe that these resources offer vast, unique, and diverse resources to the whole community.

Services include

- local area network connecting district computers by wire and wireless to district network resources and the Internet;
- videoconferencing to promote sharing of educational resources with surrounding schools and remote locations;
- computers for use by students, teachers and staff;
- voice over IP phone service;
- employee email;
- web services;
- automated dialing services for mass communication with parents;
- network printing;
- educational and productivity software;
- training on technology etiquette and appropriate behavior.

While the connection to the outside world has many benefits, there are also perils associated with the connection to the rest of the world. Sensitive information must be preserved, individual rights must be respected and the equipment must be protected from external and internal damage. APISD has taken precautions, which restrict user access to information and controversial materials as required by the Children's Internet Protection Act (CIPA). However, on a global network, it is impossible to control all materials. To maintain a healthy environment on "the network", proper conduct and strict adherence to guidelines by the end user are required. In general this requires ethical, efficient and legal utilization of the resources. Users who violate any of these provisions will be punished and may lose their account and denied access in the future. Aransas Pass ISD believes that each user should be responsible users of technology to achieve this goal each year all persons using Technology Resources at APISD will be required to review these terms and provide documentation that they agree to conform to the terms. Each campus will provide education for all students and employees about appropriate online behavior including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response as required in the Protecting Children in the 21st Center Act, Neighborhood Children's Internet Protection and Children's Internet Protection Act.

TERMS AND CONDITIONS

- 1) **CONSEQUENCES FOR REJECTION OF USER POLICY:** Network resources will be denied to any user that has not indicated they have read and agreed to the policies beginning the second week of instruction.
 - **ACCEPTABLE USE AGREEMENT:** Failure to sign or selecting the rejection statement will result in the user being blocked from all Internet resources. The user will still have access to computer resources and resources that are on the local network.
 - **DIGITAL IMAGE AGREEMENT:** Prior to having the students' image; used in a video-conference, posted on a web page or transmitted in any manner, an individual must sign and agree to this statement. ONLY a students' first name may be used on a web-site that is available outside the school district. The district will not use the web-site to post addresses or phone numbers of students.
- 2) **MONITORED USE:** You will be assigned an individual account, and you are responsible for not sharing the password or that account with others. Electronic mail transmissions and other use of the district's technology resources by students, employees, and members of the public shall not be considered private. Designated district staff shall be authorized to monitor the district's technology resources at any time to ensure appropriate use.
- 3) **ACCEPTABLE USE:** Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, Employee Handbook and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

All use of "the network" must be in support of education. Any use of "the network" for commercial or for-profit purposes is expressly prohibited.

A) **DIGITAL CITIZENSHIP** - Each user is expected to abide by the generally accepted rules of digital citizenship. These include but are not limited to:

- Be polite. Do not write or send abusive messages or materials to others.
- Use appropriate language. Do not swear; use vulgarities or other inappropriate language. Do not reveal address or phone numbers to people on the Internet.
- Immediately report communication that makes you feel uncomfortable.
- Do not use "the network" in such a way that would disrupt services to others.
- Messages relating to or in support of illegal activities may be reported to the authorities.
- All communications and information accessible via "the network" should be assumed to be public property.
- Students are not allowed to make online purchases; employees are allowed to make school purchases online.
- Not all information on the Internet is true; users are required to verify sources.
- Understand that along with technology rights comes responsibility in actions as well.

B) **SECURITY** - Users are prohibited from "hacking" or "breaching network security" of this or any other network. Any user identified as a security risk may have the account disabled. Attempting to

circumvent network security is prohibited. If you discover a possible security problem, immediately report the problem to the system administrator. DO NOT demonstrate the problem to others.

C) **COPYRIGHT** - Respect and protect the intellectual property of others. Users will not use "the network" or its components to violate the copyright of any material or download and install unapproved software. Please check the copyright rules of the materials you are using.

D) **HARASSMENT** - No user will use "the network" to send hate mail or to send messages or materials that are pornographic, derogatory or discriminatory in nature. Users should report threatening or discomfoting material including "Cyber-bullying" to the campus principal.

E) **UNACCEPTABLE AND INAPPROPRIATE USE OF TECHNOLOGY RESOURCES** - Users are prohibited from sending, posting, accessing, or displaying electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal. This prohibition applies to conduct off school property, whether the equipment used to send such messages is district-owned or personally owned, if it results in a substantial disruption to the educational environment. Any person taking, disseminating, transferring, or sharing obscene, sexually oriented, lewd, or otherwise illegal images or other content, commonly referred to as "sexting", will be disciplined according to the Employee Handbook/Student Code of Conduct and may, in certain circumstances, be reported to law enforcement.

F) **MONITORED USE** - Electronic mail transmissions and other use of the District's technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.

G) **LIMITED PERSONAL USE** - Limited personal use of the District's technology resources shall be permitted if the use:

- Imposes no tangible cost on the District;
- Does not unduly burden the District's technology resources; and
- Has no adverse effect on an employee's job performance or on a student's academic performance.

H) **EMPLOYEE USE OF ELECTRONIC MEDIA** - Refer to the APISD employee handbook section provided at end of this document titled "TECHNOLOGY RESOURCES", "PERSONAL USE OF ELECTRONIC MEDIA", and "USE OF ELECTRONIC MEDIA WITH STUDENTS".

- 4) **ELECTRONIC DEVICES AND TECHNOLOGY RESOURCES:** A user shall obtain prior approval before using personal telecommunications or other personal electronic devices for on campus instructional purposes. The user shall also acknowledge receipt and understanding of applicable regulations and shall sign the appropriate user agreements. It is the responsibility of the campus principal to set guidelines for use of the devices on the campus.
- 5) **DISCLAIMER OF LIABILITY:** The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

- 6) **SAFE USE OF EQUIPMENT:** To provide for a safe work and educational environment, always use technology equipment in a safe and appropriate manner. Electrical circuits should not be overloaded. In most areas, special power outlets are provided for computer use. DO NOT use these outlets for devices other than computers, monitors or speakers. Do not overload electrical circuits by using power strips or surge protectors. Due to the amount and function of electricity required to run laser printers, they should be on a separate circuit from computers and other technology equipment. Except in very temporary situations cables should not be run across the floor where people walk; in these cases the cords should be protected from wear with an appropriate cover and the cover should be attached to the floor to prevent tripping.
- 7) **VANDALISM:** Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data, "the network", the equipment or the software that is associated with "the network". This includes developing or loading a virus. APISD may file criminal charges on individuals that vandalize any property of APISD.
- 8) **PERSONAL INFORMATION:** Users should not give personal information (name, address, phone number...) to other online users or websites. Users should not give other student/employee information to others. Unless approved by the superintendent, no student information will be provided to outside source through electronic means. A user's directory information may be withheld at the employee's request. Users should not provide personal information to unknown sites or persons.

RECOMMENDED DISCIPLINE

- Suspension of access to the system.
- Revocation of the computer system account.
- Other disciplinary or legal action, in accordance with the Employee Handbook and applicable laws.

Technology Resources

Policy CQ

The district's technology resources, including its networks, computer systems, e-mail accounts, devices connected to its networks, and all district-owned devices used on or off school property, are primarily for administrative and instructional purposes. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district.
- Does not unduly burden the district's computer or network resources
- Has no adverse effect on job performance or on a student's academic performance

Electronic mail transmissions and other use of the technology resources are not confidential and can be monitored at any time to ensure appropriate use.

Employees are required to abide by the provisions of the acceptable use agreement and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary and legal action. Employees with questions about computer use and data management can contact Technology Department.

Personal Use of Electronic Media

Policy DH

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), web logs (blogs), wikis, electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Twitter, LinkedIn, Instagram). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic media for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.
- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, meal times, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.

- An employee may not share or post, in any format, information, videos, or pictures obtained while on duty or on district business unless the employee first obtains written approval from the employee's immediate supervisor. Employees should be cognizant that they have access to information and images that, if transmitted to the public, could violate privacy concerns.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
 - Confidentiality of student records. [See Policy FL]
 - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. [See Policy DH (EXHIBIT)]
 - Confidentiality of district records, including educator evaluations and private e-mail addresses. [See Policy GBA]
 - Copyright law [See Policy CY]
 - Prohibition against harming others by knowingly making false statements about a colleague or the school system. [See Policy DH (EXHIBIT)]

See *Use of Electronic Media with Students*, below, for regulations on employee communication with students through electronic media.

Use of Electronic Media with Students

Policy DH

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. All other employees are prohibited from communicating with students who are enrolled in the district through electronic media.

An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- The employee has provided the parent with a copy of this protocol
- The employee and the student have a social relationship outside of school;
- The parent understands that the employee's communications with the student are excepted from district regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

The following definitions apply for the use of electronic media with students:

- *Electronic media* includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), wikis, electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, Twitter, LinkedIn, Instagram). *Electronic media* also includes all forms of telecommunication such as landlines, cell phones, and web-based applications.

- *Communicate* means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee’s personal social network page or a blog) is not a *communication*: however, the employee may be subject to district regulations on personal electronic communications. See *Personal Use of Electronic Media*, above. Unsolicited contact from a student through electronic means is not a *communication*.
- *Certified or licensed employee* means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who uses electronic media to communicate with students shall observe the following:

- The employee may use any form of electronic media **except** text messaging. Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:
 - The employee shall include at least one of the student’s parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message;
 - The employee shall include his or her immediate supervisor as a recipient on each text message to the student so that the student and supervisor receive the same message; or
 - For each text message addressed to one or more students, the employee shall send a copy of the text message to the employee’s district e-mail address.
- The employee shall limit communications to matters within the scope of the employee’s professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity).
- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page (“professional page”) for the purpose of communicating with students. The employee must enable administration and parents to access the employee’s professional page.
- The employee shall not communicate directly with any student between the hours of 8:00 p.m. and 6:00 a.m. An employee may, however, make public posts to a social network site, blog, or similar application at any time.
- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators’ Code of Ethics including:
 - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. [See Policies CPC and FL]
 - Copyright law [Policy CY]
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [See Policy DF]

- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An employee may request an exception from one or more of the limitations above by submitting a written request to his or her immediate supervisor.

**ARANSAS PASS INDEPENDENT SCHOOL DISTRICT
USER AGREEMENT FORM**

Read the policy before you sign. This system was selected to provide you with the best method of customizing the use of "the network" to your needs. The signature of a parent or guardian is required for students. Select the appropriate options by initialing in the space provided. After initialing an option for each of the statements, sign and date the form at the bottom.

RESPONSIBLE USE OF TECHNOLOGY POLICY STATEMENT	Initial
I have read the Aransas Pass Independent School District Responsible use of Technology Policy and will abide by the stated terms and conditions. I understand I will be allowed to utilize network services provided by Aransas Pass Independent School District. I further understand that violation of the regulations is unethical and may constitute a criminal offense. I understand that Aransas Pass I. S. D. monitors all activities on the network. Should I commit any violation my access privileges may be revoked, disciplinary and possible legal action may be taken.	<input type="checkbox"/>
OR	
I have read the Aransas Pass Independent School District Technology Resources Terms and Conditions and do not wish to have access to telecommunication.	<input type="checkbox"/>

PHOTOGRAPH AND DIGITAL IMAGE STATEMENT	Initial
I will allow Aransas Pass to use my photograph/digital image in publications (electronic or other). Aransas Pass will use the image in an appropriate manner that actually depicts me without altering the photograph. I understand that beyond the original publication of my image, Aransas Pass Independent School District is not responsible for the use of my photograph/digital image. I further understand that Aransas Pass Independent School District reserves the right to use my photograph/digital image for future use provided it is not altered or used in an inappropriate manner.	<input type="checkbox"/>
OR	
I do not wish to have my photograph publicly used in any form.	<input type="checkbox"/>

SIGNATURES

Print User Name

User Signature

Date
