SOUTH SAN ANTONIO INDEPENDENT SCHOOL DISTRICT

Employee- Electronic Communication System Acceptable Use & Internet Safety Policy

Electronic Communication System Acceptable Use

The South San Antonio Independent School District ("South San School District" or "District") provides students and District employees access to the District's electronic networked communication system ("System"). This System includes Internet access, computer services, videoconferencing, electronic communication, computer and related electronic equipment for educational and administrative purposes. The purpose of this system is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. Additionally, the System will be used to increase District intra-communication, enhance productivity, and assist District employees in upgrading their skills through greater exchange of information with their peers. This system will assist the District in sharing information with students, employees, parents, and the local community in a responsible, efficient, ethical, and legal manner in accordance with the mission of the South San Antonio Independent School District and the Children's Internet Protection Act (CIPA - Pub. L. No. 106-554 and 47 USC 254(h) guidelines.

Electronic Communication System Access:

- The District electronic communication system has been established for educational purpose, which includes, but is not limited to promoting and enhancing classroom activities, career development, electronic communication, information sharing, and research activities.
- The District has the right to place reasonable restrictions on material that is accessed or posted throughout the system to the extent practical.
- Technology protection measures such as Internet content filters shall be in place to block or filter access to inappropriate information from Internet web pages or other forms of electronic communications. Specifically, as required by the Children's Internet Protection Act, blocking measures shall be applied to visual depictions of material deemed obscene, or child pornography, or to any other material deemed harmful to minors.
- To the extent practical, steps shall be taken to promote the safety and security of users of the District's electronic communication system when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Education of students and District employees about appropriate online behavior, including cyber bullying awareness and response, and interacting with other individuals on social networking sites and in chat rooms will occur.
- Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking', and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.
- It shall be the responsibility of all members of the South San School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.
- Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of Superintendent and/or Director of Technology or designated representatives. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.
- Use of the Internet is subject to local, state and federal laws, and use of Internet-obtained resources is in accordance with copyright law.
- Access to the District electronic communication system is a privilege — not a right. Parent/guardian permission is required for all students under the age of 18.
- It is presumed that students and District employees will honor this agreement they and/or their parent/guardian have signed. The District is not responsible for the actions of students or employees who violate them beyond the clarification of standards outlined in this policy.

- The District reserves the right to monitor all activity on this electronic communication network. Students and District employees will indemnify the District for any damage that is caused by their inappropriate use of the network.

General Unacceptable Behavior

While utilizing any portion of the South San Antonio Independent School District electronic network, unacceptable behavior by students or employees includes, but is not limited to, the following:

- Will not use the District electronic communication system to access the Internet or Intranet for any illegal activity, including violation of copyright or other contracts.
- Will not post information that, if acted upon, could cause damage or danger of disruption.
- Will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Will not knowingly or recklessly post false or defamatory information about a person or organization.
- Will not use the District equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student or District employee is told to stop sending messages, they must stop.
- Will not use criminal speech or threats to individuals or groups regarding instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Will not use speech that is inappropriate in an educational setting or violates District rules.
- Will not abuse network resources such as sending chain letters or "spamming", or forwarding such material.
- Will not waste District resources or cause unnecessary disruptions in service.
- Will not display, access or send offensive messages or pictures.
- Will not encrypt communications to avoid security review.
- Will not use the District's electronic network for commercial purposes for personal or financial gain.
- Will not attempt to gain unauthorized access to any District systems, such as student information systems, business systems, other servers, etc.
- Gaining unauthorized access to resources or information or to maliciously attempt to harm or destroy District equipment or data, or the equipment or data of any of the agencies or other networks that are connected to the Internet is strictly prohibited.
- Will not use any wired or wireless network (including third party Internet service providers by broadband cards, personal hot spots or such other devices) with unauthorized equipment brought from the outside or home, or any other device not owned by the District.
- This will be considered an attempt to bypass District filters and is considered a violation of District policy.
- Will not use District equipment, network, or credentials to threaten employees, or cause a disruption to the educational mission of the District.

E-Mail

- E-mail for district employees may be provided through a District-approved and monitored e-mail account for specific educational and work related projects or activities.
- E-mail for students may be provided through a District-approved and monitored e-mail account for specific educational projects or activities. Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

- Students will not establish or access Web-based email accounts on commercial services through the District network unless such accounts have been authorized for use by the District.
- E-mail transmissions shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use for educational, administrative or limited personal use.
- All e-mail is archived following document retention guidelines.
- The District has the right to deny the privilege of using e-mail to any user who is in violation of any guideline outlined above.
- Supervisors/Administrators have the right to request, from the Technology Department, with approval by the Superintendent or designee, copies of e-mail sent or received by students or District employee(s) if there is suspicion concerning inappropriate use.

Web Sites

- All web pages shall be school-related and will comply with federal copyright laws.
- Material placed on Web pages is expected to meet academic standards of proper spelling, grammar and accuracy of information.
- Material (graphics, text, sound, etc.) that is the ownership of someone other than the student or District employee may not be used on Web sites unless formal permission has been obtained and so noted on the page(s).
- All web pages should have a link back to the home page of the classroom, school or District, as appropriate.

System Security

- Students and District employees are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should students provide their password to another person.
- Students and District employees will not attempt to gain unauthorized access to any portion of the South San Antonio Independent School District electronic communication network. This includes attempting to login through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Students or District employees will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses, or by any other means. These actions are illegal.
- Students or District employees will not attempt to access or bypass Web sites blocked by District policy, including the use of proxy services, software, or Web sites.
- Students or District employees will not use sniffing or remote access technology to monitor the network or other user's activity.

Software and Files

- Software is available to students and District Employees to be used as an educational or administrative resource. No student or employee may install, upload or download software without permission from the District Technology Department.
- A student or District employee's account may be limited or revoked if they intentionally misuse software on any District-owned equipment.
- Students or District employees will not download or use any peer-to-peer (PTP) software, applications or websites such as Napster, Limewire, Kazza, uTorrent, etc.
- The District reserves the right to restrict the use/listening of Internet radio stations or streaming of internet video to preserve bandwidth.
- Use of computer games by students and District employees is prohibited with the exception of educational use that has been approved by the District.
- Will not download and run software such as weather and news monitoring agents, screensavers or themes that may cause performance issues or unnecessary network activity.

- Files stored on the network servers are subject to access through routine maintenance and monitoring of the South San District electronic network, and may lead to discovery that a student or District employee has violated District policy or the law. Students and District employees should not expect that files stored on District servers or computers are private.
- Personal files such as music, video, photos, images, and documents are not allowed to be uploaded and stored on the network storage provided by the district such as the network Home Drive, Google Docs, or Google Drive.

- Any malicious attempt to damage or destroy network data, resources and equipment that include but not limited to switches, wireless access points, servers, cabling and other network components connected to the network backbone, hardware or software will result in revocation of network privileges. Disciplinary measures in compliance with the District's discipline code and policies will be enforced.

Plagiarism and Copyright Infringement

- Students and District employees will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were their own.
- District policies on copyright will govern the use of material accessed and used through the District system.
- Copyrighted material will not be placed on any system without the author's permission. Permission may be specified in the document, on the system and must be obtained directly from the author.

Violations of this Acceptable Use Policy - District Employees (Consequences to violations of this policy will be handled in accordance with District disciplinary procedures and may result in any or all of the following at the Superintendent or designee's discretion):

- Immediate revocation of access to District electronic communication system with or without prior notice.
- Loss of privilege to use computer/equipment until conference held with Supervisor or designee.
- Termination of employment.
- Civil or criminal liability, including restitution, as appropriate.
- Notification of law enforcement authorities at District's discretion.

The Superintendent or designee shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

Limitation of Liability

- The District makes no guarantee that the functions or the services provided by or through the District network will be error-free or without defect. The District will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service.
- The District is not responsible for the accuracy or quality of the information obtained through or stored on the network. The District will not be responsible for financial obligations arising through the unauthorized use of the network.

The South San Antonio Independent School District Electronic Communication System Acceptable Use Policy and Internet Safety Policy were addressed at the South San Antonio Independent School District public Board Meeting on July 15, 2009.

Internet Safety Policy

1. Introduction

It is the policy of South San Antonio Independent School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h) and (i)].

2. Children's Internet Protection Act

Access to Inappropriate Material

Under the Children's Internet Protection Act (CIPA 2000), South San Antonio ISD is required to inform parents and students of the use of filtering technologies that block students' access to inappropriate web sites. To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the South San Antonio Independent School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It is the responsibility of all members of the South San Antonio Independent School District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet at all times in accordance with this policy, South San Antonio ISD Board Policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent, Director of Technology or designated representatives. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

South San Antonio ISD will monitor student use of the Internet to (a) prohibit access by minors to inappropriate material on the Internet and the World Wide Web; (b) insure the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) prohibit unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) utilize measures designed to restrict minors' access to materials harmful to minors.

South San Antonio ISD will provide age-appropriate resources and/or curriculum for students who use the school's Internet facilities that will be designed to promote the South San Antonio ISD's commitment to excellence.

- The standards and acceptable use of the Internet services as set forth in the South San Antonio ISD Internet Safety and Responsible Use Policy;
- Student safety with regard to:
    - Internet safety
    - Cyberbullying awareness and response;
    - Digital Citizenship; appropriate behavior while online, on social networking sites, chat rooms, and mobile devices.
- Compliance with the E-Rate requirements of the Children's Internet Protection Act (CIPA).
- Students will acknowledge that they received access to the resources and/or curriculum, understood it, and will follow the provisions of the district's responsible use policies.

3. Children's On-Line Privacy Protection Act

Students have the right not to give out personal information to commercial website operators as provided by The Children's Online Privacy Protection Act (COPPA), enforced by the Federal Trade Commission. Commercial website operators must get parental consent before collecting any personal information from children under the age of 13. South San Antonio ISD teachers are allowed to act on behalf of a parent and allow a student to give out personal information under COPPA.