SAN ANTONIO INDEPENDENT SCHOOL DISTRICT
Administrative Procedures

F - Students No. 26		**F26**
Page 1 of 5	Attachment(s): 1	
May 1, 2018		

USE OF COMMUNICATION TECHNOLOGIES BY STUDENTS

This Administrative Procedure defines the rights and responsibilities of both the student and the district relative to acceptable use of communication technologies. The use of technology is an important aspect of the educational experience at the San Antonio Independent School District. Communication technologies afford new and exciting learning opportunities for the student. Student use of communication technologies (whether or not owned or operated by the school district) on school grounds or at school activities is a privilege for the educational benefit of the student. Failure to adhere to these procedures may result in disciplinary action including, but not limited to, temporary or permanent loss of use of technology resources. This procedure is aligned to the Internet Safety Policies and SAISD Digital Ecosystem that offers a seamless digital environment that empowers each user with the tools needed to maximize his/her efficiency, productivity, and discovery for the highest levels of learning.

DIGITAL CITIZENSHIP

Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student behavior online are no different than face-to-face interactions.

COMMUNICATION TECHNOLOGIES

Communication technologies are comprised of the district network of wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (research databases, blogs, websites, collaboration software, social networking sites, content and learning management systems, and digital learning platforms). The district reserves the right to prioritize the use of, and access to, the network. All use of the network is consistent with the mission of the district and the alignment to the Texas Essential Knowledge and Skills (TEKS) which also promotes the development of 21st Century skills: communication, collaboration, creativity, and critical thinking necessary for college and career readiness.

STUDENT RIGHTS AND RESPONSIBILITIES

Student use of communication technologies is a privilege intended for the educational benefit of the student. Students must comply with the terms of these procedures and any applicable district Board policies and administrative procedures relative to the use of communication technologies. In using communication technologies, the student will:

1. Respect the rights of privacy of other students and district personnel
2. Remember that all student communications represent the district and thus reflect on the integrity, ethics, and good name of the district as a K-12 public education institution
3. Apply the same standards of behavior, conduct, and courtesy as are expected in the school, classroom, or other district setting
4. Comply with all laws, Board Policies, and administrative procedures regarding the use of copyrighted materials, and

5. Not seek unauthorized access to school, district, other public, or private computer networks, computers, or electronic files for any purpose

ACCEPTABLE USE

Communication technologies can be used for the creation of files, digital projects, videos, web pages, blogs and podcasts in support of education and research. Approval for these uses must be obtained as follows:

1. With the approval of the campus principal for participation in digital environments within or outside the district network such as, but not limited to, blogs, social media sites and groups, social video sharing sites, and the creation of content for podcasts, e-mail, webpages, and web conferencing.
2. With parental/guardian permission for participation in digital environments and online publication of student work, both within and outside the district network. Refer to form F26-A Communication Technologies Authorization Form for Students PreK-12. This form will default to permission to participate if not completed.

UNACCEPTABLE AND INAPPROPRIATE USE

The following forms of use of communication technologies are unacceptable and inappropriate and will be considered violations of Board Policy and Administrative Procedures. Violators will be subject to disciplinary action, including but not limited to temporary or permanent loss of use.

1. Hacking, cracking, or knowingly introducing or distributing viruses, worms, Trojan horses, time bombs or other changes to hardware, software and monitoring tools
2. Illegally installing copyrighted software for use on District computers
3. Sending messages using someone else's name or providing personal information about another individual
4. Posting, sending, or storing information online that could endanger others (i.e., bomb construction, drug manufacturing)
5. Creating or accessing messages via blogs, social media sites and groups, social video sharing sites, or creating content for podcasts, e-mail, webpages that involve Cyberbullying, hate mail, defamation, harassment or any kind of prejudicial, inflammatory or discriminatory remarks
6. Accessing, uploading, downloading, storing or distributing pornographic or sexually explicit materials that knowingly contain obscene language, graphics, pictures, or attached graphics files, either encoded/encrypted or unencoded/decrypted
7. Supporting or opposing ballot measures, candidates, or any other political activity, except when used for instructional purposes
8. Attaching unauthorized devices to the district network without principal approval. Any such device will be confiscated and additional disciplinary actions may be taken
9. Engaging in online chat sessions that are not related to coursework
10. Lending the student's account and/or password to other students and/or adults
11. Downloading, copying, duplicating or distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner
12. Publicizing the student's home address or phone number or other personal information online unless authorized by the principal for appropriate college and career opportunity Websites (i.e., College Board and FAFSA)

    Protect privacy: *Users shall be cautious about transmitting credit card numbers, account numbers of any kind, Social Security numbers, home addresses or phone numbers, or any other personal information about themselves or other individuals.*
13. Personally gaining, selling of personally owned items, commercial solicitation and compensation of any kind
14. Plagiarizing the work of others or information from any computer resource, whether from a single program or an Internet resource

INTERNET SAFETY

Personal Information and Inappropriate Content:

1. Students should not reveal personal information, including a home address and phone number on blogs, social media sites and groups, social video sharing sites, or user created content for podcasts, e-mail, webpages, and web conferencing or as content on any other electronic medium.
2. Students should not reveal personal information about another individual on any electronic medium without first obtaining permission.
3. Student pictures or names can be published on any public class, school, or district website if authorized. Refer to form F26-ACommunication Technologies Authorization Form for Students PreK-12. This form will default to permission to participate if not completed.
4. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

DIGITAL CITIZENSHIP, INFORMATION LITERACY AND CYBERSAFETY INSTRUCTION

All SAISD students will be educated about digital citizenship, information literacy, cybersafety, and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. All PreK-12 students must be taught the approved curriculum that is age appropriate and made available for use across all grade levels. Training on online safety issues and resources will be made available for administration, staff and families. Initial lessons should be conducted as soon as possible at the start of each school year and no later than the first week of October. Lessons should be implemented through both the classroom and library for new or returning students, or students who missed the initial instruction. The principal will maintain documentation that all students have received this instruction to ensure effective practices and implementation of the District's Instructional Model.

SECURITY, MONITORING AND FILTERING

Filtering software is used to block or filter access to all child pornography in accordance with the Children's Internet Protection Act (CIPA) and other objectionable material such as visual, sound or textual depictions that are obscene. The determination of what constitutes "other objectionable" material is a district decision.

1. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites. It is an expectation that the user report any instances of unblocked material within our filtering software to a teacher, administrator, or the District's Help Desk, as applicable.
2. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, virtual private networks (VPN's), https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content).
3. E-mail inconsistent with the educational and research mission of the district may be considered spam or junk mail and blocked from entering district e-mail boxes.
4. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate monitoring of student access to district devices.
5. Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district.
6. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effective and appropriate use.
7. Students and staff members may request access to Internet websites blocked by the district's filtering software. The written request will be submitted to the Office of 21st Century Learning. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request.

8. Electronic transmissions and other use of the SAISD system by students shall not be considered confidential and may be monitored at any time by designated District staff to ensure appropriate use. The district reserves the right to disclose any electronic messages to law enforcement official or third parties as appropriate.
9. In the event that the student is provided access to technology devices and software for home use, users must be aware that filtering systems are available within the SAISD network only. A parent/guardian permission form will be required for access to these devices.

DISCLAIMERS

1. SAISD makes no warranties of any kind, whether expressed or implied, for the service it is providing.
2. SAISD will not be responsible for any damages a user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions.
3. Use of any information obtained via the Internet is at the user's risk. SAISD denies any responsibility for the accuracy or quality of information obtained through its services.
4. Every user is individually responsible for his/her own actions, including, but not limited to, any monetary commitments made through an Internet communication.
5. SAISD does not condone, support, endorse, or authorize the individual actions of users of the District's communication technology resources.

DISCIPLINARY ACTIONS FOR MISUSE OR INAPPROPRIATE USE

1. **The rules listed in the USAGE RULES section of this procedure and in the *Acceptable Use of the District's Technology Resources* [FORM F26-A] are not all-inclusive, but are only illustrative and representative. Disciplinary action shall be taken for acts of misconduct listed; disciplinary action may be taken for acts of misconduct which are not specifically listed.**
2. After thoroughly investigating reported misuse, including unacceptable or inappropriate use of the Internet or any other computer resources, the principal/designee shall assign disciplinary penalties commensurate with the offense in accordance with state law, Board Policy, and the *SAISD Student Code of Conduct*. Violations of various Usage Rules are specified in the *SAISD Student Code of Conduct*. Some violations of the rules are unethical and may constitute a criminal offense. The principal/designee shall use discipline management techniques as outlined in the *SAISD Student Code of Conduct*.

STUDENT ONLINE PUBLICATION

As part of the educational experience, SAISD students can participate in digital environments using communication technologies to create files, digital projects, videos, webpages, blogs and podcasts. Parents and guardians should refer to form F26-A Communication Technologies Authorization Form for Students PreK-12. This form will default to permission to participate if not completed.

SOCIAL MEDIA – COMMUNICATION WITH EMPLOYEES

Please see Administrative Procedure D36 and Board Policy DH(LOCAL) for acceptable use guidelines on communication between students and employees via email, phone, text messaging, and social media.

STUDENT DATA IS CONFIDENTIAL

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA). To meet the FERPA requirements, any software, websites, and/or apps must first be approved for usage by the District. This applies to purchased or free content per the District's Software/App Approval Process.

DEFINITIONS

Communication Technologies – comprised of the district network of wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (research databases, blogs, websites, collaboration software, social networking sites, content and learning management systems, and digital learning platforms).

Digital Ecosystem – a framework used to interconnect digital content, technology tools, best practices, and infrastructure to offer a seamless digital environment that empowers each user with the tools needed to maximize his/her efficiency, productivity, and discovery for the highest levels of learning

Online Publications – the creation and publishing of student work within and outside the district network using online publication websites such as blogs, social media sites and groups, social video sharing sites, podcasts, e-mail, webpages, and web conferencing.

Copyrights - Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited.

Attachments: **FORM F26-A:** Communication Technologies Authorization Form for Students PreK-12

See these INDEX references for related procedures: computer use - employees

References: Board Policy CQ (LOCAL); CQ (LEGAL); ***SAISD Student Code of Conduct***

Questions regarding this procedure should be addressed to the Executive Director of the Office of 21st Century Learning, 406 Barrera Street, San Antonio, Texas, 78210/210-554-2625.