may include loss of the privilege of having a vehicle on campus. The following rules are common to parking on any school parking lot:

- **A.** All cars parked in the lot are required to have a current parking sticker;
- **B.** All traffic speed limits shall be observed;
- **C.** All traffic arrows shall be observed;
- **D.** Students are not to park in reserved or visitor parking spaces;
- **E.** No tobacco products are allowed in the parking lot;
- **F.** No alcohol or controlled substances are allowed; and
- **G.** No loitering.

26. What is Section 504?
Section 504 was derived from the 1973 Rehabilitation Act. It is defined as having a physical or mental impairment, which substantially limits one or more major life activities.

27. How does one qualify for Section 504 services?
One must have a disability that substantially impairs learning and there must be an educational need.

28. What is SISD's search process?
The district has the right and the authority to search lockers, book bags, vehicles and other items for reasons of health and safety.

29. What is SISD's process for sniff dogs?
The district has the authority to use sniff dogs to search lockers and other parts of the building and campus property.

30. What is SISD's policy on laser pointers?
Students are not permitted to possess or use laser pointers while on school property, while using district transportation, or while attending school-sponsored or school-related activities, whether on or off school property. Laser pointers will be confiscated and students will be disciplined according to the *Student Code of Conduct*.

31. If my child is accused of wrongdoing and the incident was recorded by a school video camera, will I be allowed to view the videotape?
Generally yes, you will be allowed to view the videotape but copies of the videotape might not be available to you until issues arising under the Family Educational Rights and Privacy Act (FERPA) are resolved. FERPA is a federal law which might restrict the school district's ability to share a copy of the videotape with you if it depicts other students.

32. Why is my child receiving a ticket or being punished for defending him/herself in a fight?
Self defense as use of force against another to the degree a person reasonably believes the force is immediately necessary to protect himself/herself. The privilege of self defense is limited. A claim of self defense in the use of physical force will not exempt the student from discipline when:

- The student provokes, invites or encourages the use of physical force by another person.
- The student has an opportunity to avoid physical force or to inform a school official of the threatened use of force.
- The student uses physical force after the other party abandons or attempts to abandon a fight or confrontation.

When there is a report of a fight on campus between two or more students, the school administration conducts an investigation. If the investigation reveals that the students in question have engaged in mutual combat or have intentionally or knowingly fought with another in a public place, the school administrator, dealing with the offense, will issue a consequence based on their investigation and other factors such as the students' disciplinary histories. The school administrator will also notify law enforcement. Law enforcement may also investigate the matter and issue citations or take other action that the law enforcement deems necessary.

33. What is STAAR?
STAAR is the State of Texas Assessments of Academic Readiness, the state's system of standardized academic achievement assessments, effective beginning with certain students for the 2011–2012 school year.

STAAR Alternate is an alternative state-mandated assessment designed for students with severe cognitive disabilities receiving special education services who meet the participation requirements, as determined by the student's ARD committee.

STAAR Modified is an alternative state-mandated assessment based on modified achievement standards that is administered to eligible students receiving special education services, as determined by the student's ARD committee.

STAAR Linguistically Accommodated (STAAR L) is an alternative state-mandated assessment with linguistic accommodations designed for certain recent immigrant English language learners.

APPENDIX A
SOCORRO ISD INTERNET USE POLICY

I understand and will abide by the Socorro ISD Acceptable Use Policy for Network Use. I understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and school disciplinary action may be taken. Additionally, appropriate legal action may be taken.

As the parent or guardian of this student, I have read the Socorro ISD Acceptable Use Policy for Network Access. I understand that this access is designed for educational purposes and that Socorro ISD has taken steps to eliminate controversial materials. I further understand that correct and appropriate use of the Network will be emphasized. However, I also recognize that it is impossible to restrict access to all controversial materials, and I agree that I will not hold SISD responsible for materials acquired on the Network. Further, I accept full responsibility for supervision if and when my child's internet use takes place outside of a school setting. I understand that Network access affords my son/daughter powerful opportunities and responsibilities to become a learner in the 21st century.

Parents or guardians who are interested in further information may contact the campus their child attends, or SISD's Department of Technology Services.

APPENDIX B

Student Acceptable Use Policy

Please read this Acceptable Use Policy

By Signing the Student Code of Conduct, you are acknowledging acceptance of the Student Acceptable Use Policy.

Socorro I.S.D. offers Internet access for student use. This document contains the Acceptable Use Policy for your use of the S.I.S.D. System.

A. Educational Purpose

The S.I.S.D. system has been established for an educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities.

The S.I.S.D. system has not been established as a public access service or a public forum. S.I.S.D. has the right to place reasonable restrictions on the material you access or post through the system. You are also expected to follow the rules set forth in the Student Code of Conduct (SCC), Board Policy and the law in your use of S.I.S.D.'s System

You may not use the S.I.S.D. system for commercial purposes. This means you may not offer, provide, or purchase products or services through the S.I.S.D System.

You may not use The S.I.S.D. system for political lobbying. But you may use the system to communicate with elected representatives and to express your opinion on political issues.

B. Student Network/Internet

All students will, with parental approval, have individual access to Network/Internet information resources through approved District technology devices.

Students will have e-mail access only with parental approval.

You and your parent must sign and return the Student Hand Book & Code of Conduct before access can be granted to an individual e-mail account and Network/Internet access on the S.I.S.D. system.

C. Personal Safety

- You will not post personal contact information about yourself or other people. (Examples are in: e-mail, chat rooms, personal web pages, blogs, instant messaging, etc.) Personal contact information includes, but is not limited to, your address, telephone, school address, work address, identifiable photo, etc.
- You will not agree to meet with someone you have met online without your parent's approval. Your parent should accompany you to this meeting.
- You will promptly disclose to your teacher or any other school employee any message you receive that is inappropriate or makes you feel uncomfortable.

D. Cyber Bullying

SISD prohibits the bullying of any person on school property or at school functions by use of data or computer software that is accessed through a computer, computer system, computer network or other electronic technology of the District .

Cyber Bullying means any intentional electronic act or actions against a student, school volunteer or school employee that a reasonable person, under the circumstances should know will have the effect of:

- Placing a student, school volunteer or school employee in reasonable fear of substantial harm to his or her emotional or physical well-being or substantial damage to his or her property.
- Creating a hostile, threatening, humiliating or abusive educational environment due to the pervasiveness or persistence of actions or due to a power differential between the bully and the target; or
- Interfering with a student having a safe school environment that is necessary to facilitate educational performance, opportunities or benefits; or
- Perpetuating cyber bullying by inciting, soliciting or coercing an individual or group to demean, dehumanize, embarrass or cause emotional, psychological or physical harm to another student, school volunteer or school employee

E. Unacceptable Uses

The following uses of the S.I.S.D. system are considered unacceptable:

1. Illegal Activities

- You will not attempt to gain unauthorized access to the S.I.S.D. system or to any other computer system through the District or go beyond your authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".
- You 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.
- You will not use the S.I.S.D. system to engage in any illegal act such as, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

2. System Security

- You are responsible for your individual account and should take all reasonable precautions to prevent others from being able to use your account. Under no conditions should you provide your password to another person.
- You must never use any username and/or password other than the one that is assigned to you.
- You must always log off of any computer that you have logged on to with your assigned username to prevent use by anyone else. Failure to do so may result in someone else using your username for illegal or inappropriate access. Remember, you are responsible for all activity which occurs while logged on with your username.
- You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- You will avoid the inadvertent spread of computer viruses. Students should not download software at any time unless approved by the Department of Technology Services and local school administration. Great care should be taken to keep your internet browsing to well-known high quality web sites. Do not click on unknown or suspicious links. These practices will help avoid problems with virus and malware infection on District technology devices and sytems.
- Users will not remove, disconnect, tamper with or otherwise interfere with any District computer/technology. Furthermore, no attempt will be made to bypass or uninstall any District installed software, including, but not limited to, firewalls, internet filtering, or antivirus software.
- You will not install or utilize any operating system other than the one originally installed on a District technology device. Furthermore, you will not remove an existing operating system from a District technology device.
- Users will not attempt to bypass the District Internet content filtering system in order to gain access to inappropriate or blocked sites by any means, such as, but not limited to, anonymizers or anonymous proxies and remote access programs.
- Users will not connect any computer or network devices into the District network without prior approval from the SISD Department of Technology Services.
- Users will not utilize the SISD network or technology devices illegally in ways that violate federal, state, or local laws or statutes.

3. Inappropriate Language

Restrictions against Inappropriate Language apply to public messages, private messages, and material posted on Web

- You will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- You will not post information that could cause damage or a danger of disruption.
- You will not engage in personal attacks, including prejudicial or discriminatory attacks.
- You will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If you are told by a person to stop sending messages " to them" you must stop.
- You will not knowingly or recklessly post false or defamatory information about a person or organization.
- You will not utilize the District network/internet to send anonymous email or to forge email messages to make themappeartocomefromanotherperson.

4. Respect for Privacy

- You will not repost a message that was sent to you privately without permission of the person who sent you the message.
- You will not post private information about another person.

5. Respecting Resource Limits

- You will use the system only for educational and career development activities and limited, high-quality, self discovery activities.
- You will not download large files unless absolutely necessary. If necessary, you will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to your personal computer.
- You will not use audio or video streaming unless it is for educational purposes. Overuse of these technologies causes the District network to slow down for everyone. Examples of this are: online radio and video, podcasts, etc.
- You will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

You will subscribe only to high quality discussion group mail lists that are relevant to your education or career development.

6. Plagiarism and Copyright Infringement

- You will not plagiarize works that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing. If you have questions ask a teacher.
- Downloading, copying, or installing copyrighted materials (i.e. music, movies, software, etc.) on a District computer, storing them on a District Network Share, or using a personal device on the District system to accomplish this act is unacceptable and may constitute a violation of applicable local, state, or federal law.

7. Inappropriate Access to Material

- You will not use the S.I.S.D. system to access material that is "Profane, obscene, or would embarrass or offend others around you (such as, but not limited to, graphic violence, nudity, and pornography," that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). A special exception may be made for hate literature if the purpose of your access is to conduct research and both your teacher and parent have approved.
- If you mistakenly access inappropriate information, you should immediately tell your teacher or another District employee. This will protect you against a claim that you have intentionally violated this Policy.
- Your parents should instruct you if there is additional material that they think it would be inappropriate for you to access. The District fully expects that you will follow your parent's instructions in this matter.

F. Your Rights

1. Free Speech

Your right to free speech, as set forth in the SCC applies also to your communication on the Internet. The S.I.S.D system is considered a limited forum, similar to the school newspaper, and therefore the District may restrict your speech for valid educational reasons. The District will not restrict your speech on the basis of a disagreement with the opinions you are expressing.

2. Search and Seizure

System users have no privacy expectation in the contents of their personal files on the District system. This system belongs to the School District, which has the right to access any portion of the system and any files contained in the system as authorized by the Superintendent or his/her designee.

- Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Acceptable Use Policy, District policy, Administrative Regulations or the law.
- If there is reasonable suspicion that a user has violated the law or District policy, District officials have the right to search any files or computers/technology at any time. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.
- Your parents have the right at any time to request to see the contents of your e-mail files.

3. Due Process

- The District will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the S.I.S.D system.
- In the event there is an allegation that a student has violated the District Acceptable Use Policy, the student will be afforded such rights and subject to such sanctions as set forth in District policy and the Student Code of Conduct (SCC).
- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the SCC, the violation will be handled in accord with the applicable provision of the SCC.

G. Limitation of Liability

The District makes no guarantee that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage you may suffer, 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 system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

H. Personal Responsibility

When you are using the S.I.S.D system, it may feel like you can easily break a rule and not get caught. This is not really true because whenever you do something on a network you leave little "electronic footprints," so the odds of getting caught are really about same as they are in the real world.

But the fact that you can do something or think you can do something without being caught does not make it right to do so. Even if you don't get caught, there is always one person who will know whether you have done wrong -- and that person is you. Your use of the Internet can be a mirror that will show you what kind of a person you are.