

Stockdale ISD Student Acceptable Use Policy Authorization Form

I understand that this form must be signed and returned to the School Office before my child is allowed access to District networks, computer systems and the Internet.

By signing below, I acknowledge that I have received and read the District's Student Acceptable Use Policy in the "Student Handbook" governing the use of educational technology and understand that I am obligated to become acquainted with the rules, procedures and policies outlined in the student handbook.

I certify that I understand this policy, and that I have read and reviewed it with my child and explained its implications.

I understand that I will be held accountable for my child's actions, and that disciplinary and/or legal action will result from violations of this policy.

I authorize my child to use the computers (including educational computers, the educational network, e-mail, the Internet and World Wide Web) in this school district.

Student's Full Legal Name	Campus	Grade
Parent/Legal Guardian Signature	Date	
Student Signature (Required by Sept. 1)	Date	

Stockdale ISD Student Acceptable Use Policy

Introduction

Stockdale ISD incorporates technology as a natural part of the educational process. The use of educational technology empowers students and fosters development of life-long learning skills through access to the latest equipment, information and resources.

Computers and technology are integrated into every facet of the educational and administrative process. Stockdale ISD endeavors to provide appropriate educational technology and the skills required to use this technology responsibly for all students in order to prepare them for the classroom and workplace of tomorrow.

Stockdale ISD's educational technology includes campus-wide and District-wide computer networks utilizing direct Internet access. Distance learning, streaming web-based video content, electronic mail and fax services are also available. Secure access firewalls and content-filtering software are utilized in order to protect students from inappropriate content on the Internet/World-Wide Web.

The Stockdale ISD Student Acceptable Use Policy explains and defines responsible and ethical use of educational technology for all students. All rules embodied herein guide students in appropriate and acceptable use of District technology, and are designed to protect both the student and the District. This policy also governs the use of student-owned personal electronic devices including wired or wireless desktop, portable and handheld computing devices, cameras, and cellular telephones.

Access to technology and electronic communication systems, including computer networks and the Internet, is made available exclusively for instructional purposes in accordance with District guidelines and regulations. **Access to these systems is a privilege, not a right.**

All parents/legal guardians and students on September 1st are required to acknowledge receipt and understanding of the Student Acceptable Use Policy document and must agree in writing to comply with all regulations and guidelines contained herein.

Students will not be allowed access to any educational technology or computer equipment in Stockdale ISD until their Student Acceptable Use Policy Authorization Form has been signed and returned to their school office.

Once their authorization form has been returned, each student of appropriate grade level (6th – 12th) will be issued a unique login identification code allowing access to the appropriate educational information systems. Students choose their own password.

All passwords are confidential and must not be revealed to other students.

Parents, legal guardians or students with questions or concerns regarding the Student Acceptable Use Policy should contact their campus principal or call the Stockdale ISD Technology Department at (830) 996-3551 extension 22.

Student Acceptable Use Policy

Stockdale ISD declares the following unethical and unacceptable behavior just cause for taking disciplinary action, suspending or revoking access privileges, suspending or expelling the student, and/or initiating legal action in any case in which the student:

- Uses the network and/or any attached equipment for illegal, inappropriate, subversive or obscene purposes or activities. Illegal activities shall be defined as activities violating local, state and/or federal laws, including use of the network to commit forgery, fraud or assist in the commission of a felony. Inappropriate use shall be defined as a violation of the intended educational or administrative use of the network. Subversive activities shall be defined as activities undermining the security of local, state or national governments, or activities intended to cause mental anguish, bodily injury or death to any citizen or group of citizens. Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communications vehicle, including possession or transmission of any form of pornographic or erotic material;
- Uses the network and/or any attached equipment for any illicit activity, including violation of copyrights, patents, institutional or third-party copyrights, license agreements or other contracts. Illicit activities also include transmitting or accessing information designed to aide or abet an individual or group in violating the law, including all forms of access to gang-related or organized-crime-related web sites and bulletin boards;
- Uses the network and/or any attached equipment to obtain and/or distribute illegally duplicated and distributed digital music, video and/or software from copyrighted sources. This expressly prohibits accessing “Grokster”, “Kazaa” and/or other websites and web rings designed to disseminate non-public-domain content and entertainment including, but not limited to, MP3 audio files, movies, and executable software code;
- Intentionally disrupts network traffic, deliberately “crashes” the network or connected systems or tampers with communications cabling and/or devices;
- Damages or destroys computer and/or network equipment or deliberately degrades system performance, including infection of computers or servers with viruses;
- Discloses his/her password to another student or attempts to disclose or discover another student’s or teacher’s password;
- Attempts to copy District-owned software for personal gain, attempts unauthorized transport of District-owned software beyond District boundaries, attempts to install privately-owned software onto a computer or the network or transmits any software via electronic mail or the Internet;

- Downloads, transfers or otherwise installs programs and/or files onto any computing device without teacher permission and supervision;
- Uses the Stockdale ISD network or computer resources for commercial or financial gain;
- Steals or vandalizes data, equipment or intellectual property;
- Gains or attempts to gain unauthorized access to internal and external resources or entities, including “hacking” into networks, web sites or bulletin boards;
- Forges or alters electronic mail messages or faxes, posts anonymous messages or uses an account or password owned by another user;
- Invades or assists others in invading the privacy of an individual or group;
- Possesses or conveys any data in any form including magnetic (disk/tape), optical (CD-ROM) or hardcopy (paper) which might be considered a violation of these rules.

Student Acceptable Use Policy

Once logged into the system, students will be held accountable for all activities and data transfers occurring on their computer. Any illegal or illicit use will be tracked to the student logged in. Students will be held accountable for their computer whether they or another student initiate the activity and must not let other students access their computer. **Students must properly log off the system before leaving their computer.**

Group computer usage in which multiple students simultaneously share access to a single computer is permitted only under direct teacher supervision. It is the responsibility of the teacher to monitor group activity and prevent illicit use.

Usage of Personal Electronic Devices

Students are restricted in their usage of student-owned personal electronic devices on District property and at District-sponsored events. Personal electronic devices include but are not limited to student-owned desktop, laptop, tablet and handheld computing devices, whether wired or wireless, USB drives, cameras and cellular telephones.

The following activities are regulated by the Acceptable Use Policy:

- Students are prohibited from using a camera phone (a cellular phone including a camera capable of capturing and transmitting still or full motion images) in any way that violates School or District policies, including illicit and illegal use.
- Students are prohibited from using film or digital cameras and film or digital camcorders in any way that violates School or District policies, including illicit and illegal use.
- Students may not use any personal electronic devices or media including but not limited to CD/DVD burners and USB “pen” or “jump” drives (USB keys) to

- illegally duplicate and/or distribute copyrighted materials including music, video, movies and software.
- Students may not load a bootable, alternate operating system on any District-owned computer from any student-owned source or media, including floppy disks, CD/DVD discs or USB devices (“pen” or “jump” drives (USB keys), USB hard drives or USB CD/DVD drives).
 - Students may not acquire, through wired or wireless connection, District-provided network or Internet access from any student-owned computing device whether desktop, portable, tablet or handheld, without the prior permission of their instructor and the Technology Department.

Violations of these policies will result in the immediate confiscation of the involved device(s) or media as appropriate. Depending upon the nature and severity of the violation, the confiscated device(s) or media may be held in evidence indefinitely.

Disclaimer

The District shall not be liable for any student's inappropriate use of electronic communication resources, violations of copyright restrictions, users' mistakes or negligence or costs incurred by students. The District shall not be responsible for ensuring the accuracy or usability of any information found on the Internet/World-Wide Web.

Electronic mail transmissions, faxes, and program or data files sent, received, created or accessed by students are not considered confidential and may be monitored at any time by District staff to insure appropriate use of the educational technology.

Stockdale ISD has the right to restrict or terminate Internet, network or computer access at any time for any reason. The District also has the right to monitor Internet, network and computer activity in any way necessary to maintain the integrity and security of the network and the privacy and accuracy of user information.

Consequences of Violations of the Student Acceptable Use Policy

Consequences of violations include but are not limited to:

- Suspension or revocation of Internet access privileges
- Suspension or revocation of electronic mail and/or fax privileges
- Suspension or revocation of network access privileges
- Suspension or revocation of computer access privileges
- In-school-suspension or out-of-school suspension
- District Alternative Education Program
- Expulsion
- Legal action and/or prosecution by the authorities

Remedies and Recourse

Students accused of violating the Student Acceptable Use Policy have full rights to due process and appeals as set forth in District Policy.