



Charter School *for* Applied Technologies

STUDENT ELECTRONIC AND NETWORK ACCESS ACCEPTABLE USE POLICY

CSAT is providing students access to the school's electronic network. This network includes Internet access, computer services, videoconferencing, computer equipment and related equipment for educational purposes. The purpose of this network 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. This document contains the rules and procedures for students' acceptable use of the CSAT electronic network.

- The CSAT electronic network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, career development, and limited high-quality self-discovery activities.
- The CSAT electronic network has not been established as a public access service or a public forum. CSAT has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Parent/guardian permission is required for all students under the age of 18. Access is a privilege not a right.
- It is presumed that students will honor this agreement they and their parent/guardian have signed. The school is not responsible for the actions of students who violate them beyond the clarification of standards outlined in this policy.
- CSAT reserves the right to monitor all activity on this electronic network. Students will indemnify CSAT for any damage that is caused by students' inappropriate use of the network.
- Students are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities as well as the law in the use of the CSAT electronic network.

General Unacceptable Behavior

While utilizing any portion of the CSAT electronic network, unacceptable behaviors include, but are not limited to, the following:

- Students will not post information that, if acted upon, could cause damage or danger of disruption.
- Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Students will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, they must stop.
- Students will not knowingly or recklessly post false or defamatory information about a person or organization.

- Students will not use criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Students will not use speech that is inappropriate in an educational setting or violates school rules.
- Students will not abuse network resources such as sending chain letters or "spamming."
- Students will not display, access or send offensive messages or pictures.
- Students will not use the CSAT electronic network for commercial purposes. Students will not offer, provide, or purchase products or services through this network. Students will not use the CSAT electronic network for political lobbying. Students may use the system to communicate with elected representatives and to express their opinions on political issues.
- Students will not attempt to access non-instructional school systems, such as student information systems or business systems or any other systems they are not authorized to access.
- Students will not use any wired or wireless network (including third party internet service providers) with equipment brought from home. Example: The use of a laptop computer on the network or accessing the internet from any device not owned by the school.
- Personal computer equipment is not allowed within CSAT and is not allowed to access any portion of the CSAT network.
- Students will not use school equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.
- Students will not use the school 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.

E-Mail

- High school students may be provided with CSAT e-mail accounts with the approval of the building level administrator for specific educational projects or activities.
- Students will not establish or access Web-based e-mail accounts from commercial services, such as Gmail, Yahoo etc, through the school network unless such accounts have been approved for use by the individual school.
- Students will not repost a message that was sent to them privately without the permission of the person who sent them the message.
- Students will not post private information about another person.
- All incoming and outgoing emails can be monitored at anytime and will be saved and archived for a minimum of 6 years.

Web Sites

- CSAT follows the guidelines for CIPA (Children's Internet Protection Act) for Internet Safety and in turn provides Content Filtering to block objectionable websites for all computers located within the CSAT campus.
- Access to websites for research or other educational purposes is a necessary task. Although CSAT uses Content Filtering to block certain objectionable, obscene and, violent websites etc, and non-educational websites, there is no guarantee that all websites of such manner will be blocked. CSAT employs the latest in content filtering technology but with the vast amount of websites growing every day, the ability to block all such websites is not possible. Any student who should happen to inadvertently come across a questionable website should

immediately notify their teacher or other individual who is in charge of the class at that time.

- The fact that the filtering technology has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the filtering software has protected access to certain material shall not create the presumption that the material is inappropriate for users to access.
- Websites will be monitored, and any objectionable websites found will be blocked from student access.

Personal Safety

- Students will not share personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, or work address.
- High school students will not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes, or without specific building administrative approval.
- Students will not agree to meet with someone they have met online.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.

System Security

- Students 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 must immediately notify a teacher or the system administrator if they have identified a possible security problem. Students should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Students will not attempt to gain unauthorized access to any portion of the CSAT electronic network. This includes attempting to log in 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 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.
- Users should immediately notify a network administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk will have limitations placed on usage of the network or may be terminated as a user and be subject to other disciplinary action.
- Users will not attempt to access Web sites blocked by school policy, including the use of proxy services, software, or Web sites.
- Users 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 to be used as an educational resource. No student may install, upload or download software without permission from the CSAT technology department.
- A student's account may be limited or terminated if a student intentionally misuses software on any school-owned equipment.

- Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of the CSAT electronic network may lead to discovery that a student has violated this policy or the law. Students should not expect that files stored on school servers are private.

Technology Hardware

- Hardware and peripherals are provided as tools for student use for educational purposes.
- Students are not permitted to relocate hardware (except for portable devices), install peripherals or modify settings to equipment without the consent of the CSAT technology department.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the school's discipline code and policies will be enforced.

Plagiarism and Copyright Infringement

- Students will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were the students'.
- CSAT policies on copyright will govern the use of material accessed and used through the school 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 or must be obtained directly from the author.

Videoconference

- Videoconferencing is a way that students can communicate with other students, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, students can see, hear, and speak with other students, speakers, museum personnel, etc. in real-time.
- Videoconference sessions may be videotaped by school personnel or by a participating school involved in the exchange in order to share the experience within ours or their building or school.
- Students' voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Rules and procedures relative to acceptable use and behavior by students apply during all videoconference sessions.

Student Rights

- Students' right to free speech applies to communication on the Internet. The CSAT electronic network is considered a limited forum, similar to the school newspaper, and therefore the school may restrict a student's speech for valid educational reasons. The school will not restrict a student's speech on the basis of a disagreement with the opinions that are being expressed.
- An individual search will be conducted if there is reasonable suspicion that a student has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

Due Process

- CSAT will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the school network.
- In the event there is an allegation that a student has violated the CSAT acceptable use regulation and policy, the student will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation before a school administrator (or student will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code).
- 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. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.
- If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of his/her network account.

Limitation of Liability

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

Violations of this Acceptable Use Policy

Violations of this policy may result in loss of access as well as other disciplinary or legal action. Students' violation of this policy shall be subject to the consequences as indicated within this policy as well as other appropriate discipline, which includes but is not limited to:

- Use of school network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school and/or
- Legal action and prosecution by the authorities

The particular consequences for violations of this policy shall be determined by the school administrators. The superintendent or designee and/or the board shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.