



Student Acceptable Use Policy

The Crandall Independent School District provides a variety of electronic communications systems for educational purposes. **The electronic communications system is defined as the District's network (including the wireless network), servers, computer workstations, mobile technologies, peripherals, applications, databases, online resources, Internet access, email, and any other technology designated for use by students, including all new technologies as they become available.** This also includes any access to the Crandall ISD electronics system while on or near school property, in school vehicles and at school-sponsored activities, and includes the appropriate use of district technology resources via off-campus remote access. Please note that the Internet is a network of many types of communication and information networks, including Digital resources, and is part of the district's electronic communications systems. Digital applications offer a variety of communication, collaboration, and educational creativity opportunities.

In accordance with the Children's Internet Protection Act, Crandall Independent School District educates staff and students regarding appropriate online behavior to ensure Internet safety, including use of email and online resources, and has deployed filtering technology and protection measures to restrict access to inappropriate content such as those that are illegal, obscene or harmful to minors. While every effort is made to provide the most secure and optimal learning environment, it is not possible to absolutely prevent access (accidental or otherwise) to inappropriate content. If you come across any inappropriate content or communication notify a teacher or parent immediately. **It is each student's responsibility to follow the guidelines for appropriate and acceptable use.**

Appropriate Use

- Students must only open, view, modify, and delete their own computer files.
- Internet use in the classroom must be directly related to school assignments and projects
- Students will be assigned individual email and network accounts and must use only those accounts and passwords that they have been granted permission by the district to use. All account activity should be for educational purposes only.
- Students must immediately report threatening messages or discomfoting Internet files/sites to a teacher.
- Students must at all times use the district's electronic communications system, including email, wireless network access, and digital tools/resources to communicate only in ways that are kind and respectful.
- Students are responsible at all times for their use of the district's electronic communications system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them freedom to do otherwise.
- Students who choose to use their own personal device in lieu of a district issued device will use the CISD byod network for filtering purposes.



Inappropriate Use

- Wireless Hotspots not provided by CISD are prohibited on the CISD network.
- Using the district's electronic communications system for illegal purposes including, but not limited to, cyberbullying, gambling, pornography, and computer hacking.
- Disabling or attempting to disable or bypass any system monitoring or filtering or security measures, including deleting browser history to conceal Internet patterns.
- Sharing user names and passwords with others; and/or borrowing someone else's username, password, or account access.
- Purposefully opening, viewing, using or deleting files belonging to another network user without permission.
- Electronically posting personally identifying information about one's self or others (i.e. addresses, phone numbers, and pictures).
- Downloading or plagiarizing copyrighted information without permission from the copyright holder.
- Intentionally introducing a virus or other malicious programs onto the district's network.
- Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Gaining unauthorized access to restricted information or network resources.

Cyberbullying

Cyberbullying is defined as the use of any Internet-connected device for the purpose of bullying, harassing, or intimidating another student. This includes, but may not be limited to:

- Sending abusive text messages to cell phones, computers, or Internet-connected game consoles.
- Posting abusive comments on someone's blog or social networking site (e.g., Instagram or Facebook).
- Creating a social networking site or web page that masquerades as the victim's personal site and using it to embarrass him or her.
- Making it appear that the victim is posting malicious comments about friends to isolate him or her from friends.
- Posting the victim's personally identifiable information on a site to put them at greater risk of contact by predators or strangers.
- Sending abusive comments while playing interactive games.
- Recording and distributing media with the intent to manipulate or embarrass others.

Children's Online Privacy Protection Act (COPPA)

Students 13 or younger. For students under the age of 13 the Children's Online Privacy Protection Act requires additional parental permission for education software tools that collect personal information about the child. Parents wishing to deny access to these educational tools must do so in writing to the campus principal.



Children's Internet Protection Act (CIPA)

All students will receive training in compliance with the CIPA. Training will address:

- Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use and dissemination of personal information regarding minors;
- Measures designed to restrict minors' access to materials harmful to minors; and
- Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

Consequences of Inappropriate Use

- Appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws including monetary damages.
- Suspension of access to the district's electronic communications system.
- Revocation of the district's electronic communications system account(s); and/or
- Termination of System User Account: The district may deny, revoke, or suspend specific user's access to the district's system with or without cause or notice for lack of use, violation of policy or regulations regarding acceptable network use, or as a result of disciplinary actions against the user.
- Possible criminal action.

Bring Your Own Device

It is our goal that students and teachers will collaborate in rich, engaging learning experiences using technology. Students may bring their own technology and utilize personal electronic communication devices at school and at school activities. Students may use these devices in the classroom when the teacher deems them appropriate for educational purposes. All devices must remain silent or be put away unless being used within a lesson during class time. Students may also use devices during non-instructional times, such as passing periods, lunch and before/after school.

Devices should be clearly labeled with the student's full name. Students are responsible for personal property brought to school and should keep personal items with self or in a locked space. Devices should be charged prior to bringing them to school.

In the event the technology is used inappropriately, disciplinary consequences as outlined in the Student Code of Conduct may occur.



Disclaimer

The district's system is provided on an "as is, as available" basis. The district does not make any warranties, whether expressed or implied, including, without limitation, those of fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The district uses a variety of vendor-supplied hardware and software. Therefore, the district does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the user's requirements. Neither does the district warrant that the system will be uninterrupted or error-free, nor that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not necessarily the district.

The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's computer systems and networks.

Google Services

Crandall ISD licenses a Google Workspace for Education Account for every student, which will include the core Google Services and additional services based on curriculum requirements and grade level.

Term

This policy is binding for the duration of the student's enrollment in CISD.



Crandall ISD STUDENT AUP AGREEMENT

Student ID:

Grade:

School: _____

I understand that my computer use is not private and that the District will monitor activity on the computer system. I have read the District's electronic communications system policy and administrative regulations and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access.

Student First Name (Please print)

Student Last Name (Please print)

Student Signature

Date (mm/dd/yyyy)

PARENT AGREEMENT:

I have read the District's Guidelines for Acceptable Use of Crandall Independent School District Technology Resources, and this agreement form. In consideration for the privilege of my child using the District's electronic communications system, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the type of damage identified in the District's policy, and administrative regulations.

Parent or Guardian Name – (Please print)

Parent or Guardian Signature

Home address

Home phone number

Email address

Date (mm/dd/yyyy)

