

Caldwell Independent School District Internet Safety/Acceptable Use Policy

Adopted by the Board of Trustees for Caldwell Independent School District
at a public meeting, following normal public notice on June 28, 2010.

OVERVIEW

The Caldwell Independent School District (CISD) has made Internet access available to students and staff in the district. We are very pleased to bring this access to CISD and believe the Internet offers vast, diverse, and unique resources to both students and staff. Our goal is to promote educational excellence in schools by facilitating resource sharing, innovation, and communication through technology. Students have access to the Internet as a means to enhance their education.

We live in a rapidly, changing world, where continuous access to information is evolving faster than ever before. Students and staff now can be both consumers and producers of information, and the District strives to be a 21st Century district taking advantage of the many new technologies and new methods of communication now available to our district.

We are trying to create an environment that provides guidelines for our students and staff to use new technologies in a meaningful way and to embrace them in ways that align to the ISTE National Education Technology Standards (NETS). With access to these new technologies, students will have opportunities to learn and create like never before, but with those opportunities, new responsibilities appear.

CISD does not have complete control of the information on the Internet even though a filtering system is in place. Some sites accessible via the Internet may contain materials that are inappropriate for K-12. With new websites being launched every day, it is possible that any filtering system would not be one hundred percent preventative. CISD and the Technology Department do not condone the use of inappropriate materials and do not permit usage of such materials in the school environment.

Our district provides an array of technology resources for district use. This agreement outlines used and prohibited activities when using technologies resources. Every member of this district is expected to follow all guidelines stated below, as well as those given orally by the staff, and to demonstrate good citizenship and ethical behavior at all times.

In accepting this agreement, district users acknowledge the following rules and conditions:

As a District user, I understand that my school network and email accounts are owned by the District and are not private. CISD has the right to access my information as any time.

DISCLAIMER

Access to the Internet is provided on an "as is, as available" basis. The district makes no warranties of any kind, where expressed or implied, for the services it is providing and is not responsible for any damages suffered by users. This includes loss of data resulting from delays, non-deliveries, miss-deliveries, or service interruptions caused by its negligence or user errors or omissions. In the process of protecting the network, CISD cannot guarantee the confidentiality of information. Use of any information obtained via the Network/Internet is at the user's own risk. CISD specifically denies any responsibility for the accuracy or quality of information obtained through its Internet accounts.

Further, CISD denies any responsibility for liability of purchases resulting from use of its Internet accounts. Opinion, 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 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 Network/Internet/Electronic communications systems.

ELECTRONIC COMMUNICATIONS NETWORK/ACCEPTABLE USE POLICY

The district network is a primary source for voice, video, and data transmission, communication, storage, and application delivery. The Internet is a primary source for research, information, and communication. Access to the Internet is provided to CISD employees in order to take advantage of innovative instruction methodology and workplace technological advancements. Access to the Internet is also provided to CISD students in order to fulfill their potential as responsible citizens in the ever changing world of the 21st century. Along with this privilege come responsibilities.

CISD reserves the right to audit network and systems on a periodic basis to ensure compliance with the agreement and all associated policies. Any employee found in violations of this agreement can be subjected to disciplinary action up to and including termination of employment and legal prosecution.

Caldwell is pleased to offer technological opportunities to our students, staff, and administrators. With the Internet a primary source for research, information, and communication, access to the Internet is provided for instructional and administrative purposes consistent with the District's mission and goals.

In compliance with the Children's Internet Protection Act (CIPA), CISD's Internet access includes filtering and/or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or similar materials considered harmful to minors. Content will be filtered for both minors and adults. Unfortunately, there is not a system that will provide 100% protection from inappropriate material; therefore, it is possible that users may run across areas of adult content and/or material that might be found objectionable. The Internet is a primary source for research, information and communication.

ELECTRONIC COMMUNICATION

The District e-mail system is used to communicate internally in the District and with outside agencies. E-mail communications are a matter of public record and should not be considered confidential and may be monitored at any time by designated staff. All users are expected to adhere to the following District policies regarding e-mail communications.

- E-mail should not be used for private or commercial offering of products or services for sale or to solicit products or services.
- E-mail should not be used for political or religious purposes.
- Forgery or attempted forgery of electronic mail is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other users, deliberate interference with the ability of other users to send/receive electronic mail, or the use of another person's ID and/or password is prohibited.
- Chain mail, e-mails that "must be forwarded x number of times", and other unsolicited junk email is prohibited.
- E-mail messages that cause network congestion or interfere with the delivery of mail to others are not acceptable.
- E-mail messages and forums posting will not contain improper language, swearing, vulgarity, ethnic or racial slurs or any inflammatory language or content.
- Do not reveal personal information about yourself or others.
- Do not send chain letters, or forward messages to large groups of users.
- You are expected to be polite and professional.
- You are responsible for material sent by and delivered to your e-mail account.
- E-mail communications are retained on the network server for 30 days.
- District e-mail should be used primarily for educational/district related purposes.
- Use appropriate language and follow proper e-mail etiquette.

- If you receive an inappropriate or unwanted message, close the mail and notify appropriate administrative staff.

NETWORK USER ACCOUNTS

The Caldwell ISD network and Internet services are not private. Data and/or users may be monitored by the CISD Technology Department and/or CISD administrators at any time to ensure proper use. The Internet may not be accessed by a student until an Internet Safety/Acceptable Use Policy is signed according to policy and returned to the campus. This request, indicating that the Internet may be accessed, must be filed annually.

While using networked resources,

- Students in kindergarten through twelfth grades will be assigned an individual account for system access.
- All staff members will be assigned an individual account for system access. The district will require staff passwords to be changed on a regular basis.
- Do not make your password available to others.
- Do not login using an unauthorized account, another user's account, or allow students to access an employee's account.
- Do not leave your computer unattended. If you must leave your computer for a moment, either log off or lock the computer. Always log off when you are finished.
- Do not view, modify, move, copy or delete folders or files unless given permission by a teacher or other CISD employee.
- Do not waste or monopolize network resources
- Do not connect any personal devices, other than external storage drives, to the district network.
- Employees shall only access applications, reports, data, that are pertinent to their job responsibilities. The Network Administrator establishes permissions and security profiles for all employees; however, conflicts sometime occur. Please notify the Technology Department if you find potential permissions errors.
- Certain positions within district require access to confidential information. All district policies regarding confidential information must be adhered to through network and electronic communications.
- Do not use the network for unauthorized access, (hacking) of web sites and password-protected folders.
- Do not use for illegal purposes, in support of illegal activities, or for any other activity prohibited by district policy.
- Do not use for commercial, income-generating or "for profit" activities, product advertisement, or political lobbying is prohibited.
- The user is responsible at all times for the proper use of his/her account.

INTERNET USE

Only access the Internet with permission and under the supervision of a teacher or other CISD employee.

- Before downloading files or running programs from the Internet or changing computer settings/properties, obtain permission of a teacher or other CISD employee
- Follow Copyright Laws and Fair use guidelines.
- Use of the Internet by students must be supervised.
- The Internet should be used primarily for educational/district related purposes. All activity on the Internet is being recorded and can be monitored. Limited personal use shall be permitted if the use:
 - Imposes no tangible cost to the District;
 - Does not unduly burden the District's computer or network resources;
 - Has no adverse effect on an employee's job performance or on a student's academic performance; and/or

- Is not used in any way for personal gain.

WEB PAGES

The District will maintain a District Web site for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District Web site must be directed to the designated Webmaster. The Superintendent and Director of Technology will establish guidelines for the development and format of Web pages controlled by the District.

No personally identifiable information regarding a student will be published on a Web site controlled by the District without written permission from the student's parent. No commercial advertising will be permitted on a Web site controlled by the District.

Schools, classes, and extra-curricular organizational web pages may create pages that present information about their school, class and/or organization. Those having web pages will be in compliance with District rules for maintaining the Web page.

USE OF NEW WEB TOOLS

Online communication is critical to our students' learning of 21st Century Skills and Social Networking sites offer an authentic, real-world vehicle for student expression. Again, as educators, our primary responsibility to students is their safety. Hence, expectations for classroom Web interactive use must follow all established Internet safety guidelines.

- The use of blogs, podcasts or other web 2.0 tools may be considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes but is not limited to profanity; racist, sexist or discriminatory remarks. Students using blogs, podcasts or other web tools are expected to act safely by keeping **ALL** personal information out of their posts.
- Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a school setting.
- Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat these tools as classroom spaces. Speech that is inappropriate for class is also inappropriate.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in projects and/or be subject to consequences appropriate to misuse. If caught in an act of inappropriate use of social networking sites, the student will be punished according to the Student Code of Conduct.

CELLULAR TELEPHONE AND ELECTRONIC SIGNALING DEVICE POLICY

Student possession and use of cellular phones, pagers and other electronic signaling devices on school campuses and school buses, at school sponsored activities, and while under the supervision and control of school district employees is permitted under circumstances described herein.

Students are permitted to bring cell phones to school. The purpose of allowing students to bring cell phones to school is to ensure they are available for after school use only. All students (K-12) may use these devices on campus before school begins and after school ends.

These devices must be kept out of sight and turned off during the instructional program and in the classroom. Cell phones may be used for educational purposes under the direct supervision of the teacher for classroom use only. Unauthorized use of these devices disrupts the instructional program and distracts from the learning environment. School officials, including classroom teachers, may take the device away from students if used during the times not permitted. Repeated unauthorized use of such devices may lead to disciplinary action.

If caught in an act of inappropriate use of an electronic device, the student will be punished according to the Student Code of Conduct.

CISD is not responsible for any lost, stolen or damaged cell phones and/or electronic signaling device.

COPYRIGHT

Copyrighted software or data may not be placed on any system connected to the District's system(s) without permission from the holder of the copyright. Only the owner(s) or individuals the owner(s) specifically authorized may upload copyrighted material to the system(s).

CONSENT

No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent if the student is a minor) or employee who created the work. At no time will both student picture and full name be posted together.

No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent. An exception to this rule may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and District policy.

VIOLATIONS

Any malicious attempt to harm or destroy District equipment or data or the data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences.

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

CONSEQUENCES

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the Principal or Director of Technology receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.