

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT
Crane ISD 2008-2009 Acceptable Use Policy

CQ (LOCAL)

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

USE BY MEMBERS OF THE PUBLIC

Access to the District's electronic communications system, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the District; and
2. Does not unduly burden the District's computer or network resources.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy. Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

FILTERING

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

MONITORED USE

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered private. Designated District staff shall be authorized to monitor such communication at any time to ensure appropriate use.

**INTELLECTUAL
PROPERTY
RIGHTS**

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

**DISCLAIMER OF
LIABILITY**

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

End of CQ (LOCAL)

GENERAL DISTRICT RESPONSIBILITIES

The Superintendent or designee will oversee the District's electronic communications system and work with the Regional Educational Service Center and TEA network staff, as appropriate.

Commercial use of the District's network system is strictly prohibited.

Copyrighted software or data may not be placed on any system connected to the District's network system without the author's permission. Only the owner(s) or individuals the owner specifically authorizes may upload copyrighted material to the system.

Unless required to do so by law or by policies of the District or to investigate complaints regarding electronic mail that is alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, offensive, or illegal material, the system administrator will not intentionally inspect the contents of electronic mail sent by a system user to an identified addressee or disclose such contents to anyone other than the sender.

SYSTEM ACCESS

All users of the District's network system will be provided with a user name and password. The user is responsible for maintaining the security of his/her password. The Superintendent or designee may require that passwords be changed periodically to maintain a reasonable level of security.

Any system user identified as a security risk or having a history of violations of District and/or campus computer use guidelines may be denied access to the District's network system.

SYSTEM ADMINISTRATOR RESPONSIBILITIES

The system administrator will:

1. be responsible for disseminating and enforcing District policies and administrative regulations governing use of the District's network system.
2. ensure that system users have been provided appropriate training.
3. be authorized to monitor or examine all system activities as deemed appropriate to ensure proper use of the system.
4. be authorized to establish a retention schedule for electronic messages on the system.
5. set quotas for disk usage on the system, as needed. Requests for increased quotas may be submitted to the system administrator and should state the reason for the requested increase.

6. ensure that all users of the District's network system sign an agreement to abide by the District's policies and administrative regulations regarding such use. All such agreements will be maintained and filed in the appropriate office.

INDIVIDUAL USER RESPONSIBILITIES

The following rules will apply to all users of the District's electronic information/communication systems:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use. If the user believes that his/her password has been compromised, it is the user's responsibility to report any inappropriate activities that resulted from the breach and to change the password on the account to re-establish account security. All security problems in the District's system must be reported to the appropriate teacher or administrator as appropriate.
2. System users must not encourage the use of alcohol, tobacco, or controlled substances or otherwise promote any activity prohibited by District policy or state or federal law.
3. Transmission of material, information, or software in violation of any District policy or local, state, or federal law is prohibited.
4. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
5. System users may not use another person's system account. Attempting to log on to the District's network system as another user may result in cancellation of user privileges and/or other disciplinary action.
6. System users may not post messages or access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal. The Internet filtering process cannot filter ALL inappropriate material. The user is not permitted to access inappropriate material even if the filter would allow it.
7. A student may use real-time conference features such as talk/chat/Internet relay chat only as approved by the supervising teacher. All such activities must be monitored by the supervising teacher.
8. System users must remove electronic mail in accordance with established retention guidelines. Messages may be removed by the system administrator if guidelines are not followed by the user.
9. System users will not disable virus protection on any part of the system. Real-time virus protection must be in place at all times.
10. System users must not evade or otherwise manipulate the filtering process for Internet access that is maintained by the District. Use of peer-to-peer file sharing processes (on the local area

network as well as across the Internet) are strictly prohibited without permission from the system administrator.

11. System users must abide by copyright regulations concerning downloaded material as well as any software that is to be installed on a District computer.

12. System users who have Internet filter bypass authorization must maintain the security of such access and monitor all access to the system while the bypass is in place.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or materials, data of another user or the District's system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance will be viewed as violations of District policy and may be viewed as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses. Any interference with the work of other users, including erasing, renaming or making files or disks unusable, with or without malicious intent, is construed as mischief and is strictly prohibited. Vandalism of this nature may result in the cancellation of system use privileges and could result in restitution for costs associated with system restoration, hardware, or software costs.

FORGERY PROHIBITED

Forgery or attempted forgery of electronic mail messages or other data on the network system is prohibited. Attempts to read, delete, copy or modify the electronic mail or other data of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

INFORMATION CONTENT / THIRD PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

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

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

System users may order services or merchandise from individuals and agencies not affiliated with the District but may be accessed through the District's system. All matters concerning merchandise and services ordered including, but not limited to, purchase terms, payment terms, warranties and guarantees, and delivery are solely between the seller and the system user. The

District makes no warranties or representation whatsoever with regard to any goods or services provided by the seller and the system user. The District makes no warranties or representation whatsoever with regard to any goods or services provided by the seller.

District employees and administration will not be party to any such transaction or be liable for any costs or damages arising out of either directly or indirectly, the actions of inactions of sellers.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon any violation of district policy and/or administrative regulation.

Prior to a suspension or revocation of system service, or as soon as practicable, the principal or other supervisor will inform the system user of the suspected violation and give him/her an opportunity to present an explanation, as follows:

1. A system user may appeal the suspension or revocation within seven calendar days.
2. The District coordinator or designee will conduct hearing before a committee. The person who imposed the suspension or revocation will not be assigned to the committee hearing the appeal.

Termination of an employee's account will coincide with the effective date of resignation or termination of employment. Termination of student's access will be effective on the date the principal receives notice of student withdrawal or revocation of system privileges, or on a future date of so specified in the notice.

Teacher Web Page Guidelines

Protocol and Responsibility

1. Each teacher is responsible for the development and maintenance of his or her pages. The Technology Department will offer training and support for staff members.
2. Each campus is responsible for acquiring the CISD Publications, Video, Internet Consent and Release Agreement prior to posting any student's picture, art work, written work, voice, verbal statements or portraits (video or still) on the school's web pages. This form must be signed by the parent(s) and filed at the campus office.
3. When using the OnCourse system, teachers will have the ability to create and post pages with no intervention by any administrative personnel. Therefore, teachers are responsible for following these guidelines for all web pages under their supervision.

Requirements

1. All pages should be checked for grammatical and spelling errors. Content should be worthwhile. Emphasize content over glitz.
2. Pages that contain time-sensitive information such as calendars, school events, staff information must be updated monthly to ensure current, accurate information.
3. Web pages must be checked monthly to make sure that all links work.
4. The Crane ISD website is for educational use only. Contents of the site should provide school-related information and promote school activities (PTSA, classes, staff, departments, sports, school projects, calendars, volunteering opportunities, etc.). Web pages should not include personal expressions of a religious or political nature. Information concerning non-curricular student groups may be posted if the pages meet all district requirements and a school employee/sponsor has approved the pages.
8. External Links (Links to sites and content that is not hosted on the Crane ISD web server or the OnCourse system)
 - a. Commercial Links that are related to fundraising opportunities may be allowed with approval from the superintendent, campus principal or the technology director. Any other commercial transactions or advertisements are prohibited on school pages.
 - b. Educational Links are allowed on pages if the site is curriculum content focused and not primarily commercial content and is appropriate in a school setting. Sites that contain advertising should have the following statement beside the link: Note: Site contains advertising.
 - c. NOTE: In all cases where an external link is used on a school web page, the following disclaimer statement must be present on the teacher or school's main navigation page. Crane ISD is not responsible for contents on external sites or servers.
9. Files hosted on the Crane ISD web servers and hyperlinks from these files should not contain directory information that is in violation of (or promotes the violation of) any district policy or regulation nor any local, state or federal regulation or law.
10. The following student directory information is generally acceptable to include, if the consent form has been signed, on a school web page.
 - a. Elementary students: Student's picture or work with first name or first name and last initial only.
 - b. Secondary students: Student's picture or work with first name and last name or first name and last initial or first name.
 - c. No other personal information about a student is allowed such as email address, phone number or home address.
11. Unauthorized use of copyrighted material is prohibited. Giving credit (web address or active link) to company that has created a graphic, design, etc. for a school page may be allowed, unless the internet filter blocks the site.
12. **Prohibited** items include:

- a. Personal information about staff and parent volunteers: non-district email addresses, non-district mailing address and non-district phone numbers except as approved by your administrator. Example: PTSA/Booster Organization officer/contact requests to have their personal email address listed in the appropriate area on the school's page(s) and the superintendent, your principal or the technology director approves the request. Note: Pictures and names of staff and parent volunteers will be allowed with the Web Page committee's approval.
- b. Student personal contact information of any kind.
- c. Links to staff, volunteer or student personal home pages.
- d. Links to "non-official" Crane ISD related sites that are hosted on remote/external (non-district) web servers – Examples: athletic booster pages, PTSA pages, teacher created classroom pages, etc. However, booster organizations, PTSA, teachers, etc. may post their pages on the district's Web site following the same protocol and guidelines presented in this document.
- e. "Guest books", "chat areas", "message boards" or similar areas.
- f. Links to sites that are not accessible inside the network (through the internet filter).