
The Superintendent or designee will oversee the district's electronic communications system.

The district will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines (Exhibit A). All training in the use of the district's system will emphasize the ethical and safe use of this resource.

**CONSENT
REQUIREMENTS**

Copyrighted software or data may not be placed on any system connected to the district's system without permission from the holder of the copyright. Only the copyright owner, or an individual the owner specifically authorizes, may upload copyrighted material to the system.

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.

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 may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act and district policy.

FILTERING

A committee, chaired by the Associate Superintendent for Technology & School Services or designee, will select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.

The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to: nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and on-line gambling.

**REQUESTS TO
DISABLE FILTER**

The committee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes. The committee will make recommendation to the Superintendent regarding approval or disapproval to disable the filter for the requested use.

SYSTEM ACCESS

Access to the district's electronic communications system will be governed as follows:

1. All users will be required to acknowledge their receipt and understanding of the acceptable use guidelines as published in the Student Handbook and Code of Conduct for students and the Employee Handbook for employees.
2. 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 by employees shall be permitted if the use:
 - a. Imposes no tangible cost on the district;
 - b. Does not unduly burden the district's computer or network resources; and
 - c. Has no adverse effect on an employee's job performance.
3. Students will be granted access to the district's system and will be assigned individual accounts.
4. As appropriate, district employees will be granted access to the district's system.
5. The district will require that all passwords be changed every 90 days.
6. Any system user identified as a security risk or as having violated district and/or campus computer use guidelines may be denied access to the district's system.

TECHNOLOGY COORDINATOR RESPONSIBILITIES

The Associate Superintendent for Technology & School Services or designee for the district's electronic communications system (or campus designee) will:

1. Be responsible for disseminating and enforcing applicable district policies and acceptable use guidelines for the district's system.
2. Ensure that all users of the district's system complete and sign annually an agreement to abide by district policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's or supervisor's office.
3. Ensure that employees supervising students who use the district's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the district is consistent with district standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure student safety on-line and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.
7. Set limits for data storage within the district's system, as needed.

**MONITORED USE,
EMAIL, CHAT
ROOMS**

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use for educational or administrative purposes. Suspected violations of acceptable use by employees should be reported to the Assistant Superintendent for Human Resources. Suspected violations of acceptable use by students should be reported first to the campus principal and, if necessary, by the campus principal to the Assistant Superintendent for Student Services.

The district does not provide student electronic mail accounts. No participation in any chat room (or newsgroup) accessed on the Internet is permissible for students or employees.

**DISTRICT
WEB SITE**

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 Assistant Superintendent for Communication or designee. The Associate Superintendent for Technology & School Services or designee and the Assistant Superintendent for Communication or designee will establish guidelines for the development and format of Web pages controlled by the district.

Regarding student information published on a Web site controlled by the district, see Exhibit A.

**SCHOOL OR CLASS
WEB PAGES**

Schools may publish Web pages that present information about school activities, subject to approval from the Assistant Superintendent for Communication or designee, and link to the district's site. The campus principal will designate the staff member responsible for managing the campus' Web page under the supervision of the Assistant Superintendent for Communication or designee. Any links from a Web page to sites outside the district's computer system must receive approval from the Assistant Superintendent for Communication or designee.

**PERSONAL WEB
PAGES**

District employees, trustees, and members of the public may not be permitted to publish personal Web pages using district resources.

**NETWORK
ETIQUETTE**

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.

4. Transmitting obscene messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

**TERMINATION /
REVOCATION OF
SYSTEM USER
ACCOUNT**

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 Associate Superintendent for Technology & School Services or designee receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

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 merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. 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 system user's requirements, or that the system will be uninterrupted or error free, or 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 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 electronic communications system.

Cypress-Fairbanks Independent School District
Network/Internet Acceptable Use Guidelines

Network/Internet access is available to students, teachers and staff in the Cypress-Fairbanks Independent School District (“the district”). The Internet is a network connecting millions of computer users all over the world. The Internet enables worldwide connections to electronic mail, discussion groups, databases, software, and other information sources, such as libraries and museums. The district provides Network/Internet access to promote educational excellence in the district by facilitating resource sharing, innovation, and communication. The district firmly believes that the valuable information and interaction available on the Network/Internet far outweighs the possibility that users may procure material that is not consistent with the educational goals of the district.

Network/Internet - Terms and Conditions

Training:

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the district's system will emphasize legal, ethical, and safe use of this resource.

Risk:

Sites accessible via the Network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. **Although the district will attempt to limit access to objectionable material by using filtering software, controlling all materials on the Network/Internet is impossible.** With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Monitored Use:

Electronic mail transmissions and other use of the electronic communications system by students and employees shall not be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use. This monitoring may include activity logging, virus scanning, and content scanning. The district does not provide student electronic mail accounts and specifically prohibits student participation in chat rooms while using school equipment, including computers.

The district has provided students with access to “Digital Lockers,” a network storage location for files. The “digital locker” provides an area where certain school-related student products can be stored from year to year, thus creating the student digital portfolio.

To enforce the Student AUP and to maintain the integrity of the network, digital lockers will be monitored by district staff and files such as games, inappropriate images and files will be deleted. Student disciplinary action may follow.

User Responsibilities:

Network/Internet users, (students and district employees), like traditional library users or those participating in field trips, are responsible for their actions in accessing available resources. The following standards will apply to all users (students and district employees) of the Network/Internet:

1. The user in whose name a system account is issued will be responsible at all times for its proper use. Users may not access another person's account without written permission from a campus administrator or district level administrator.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by district policy.
3. Users may not redistribute copyrighted programs or data without the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, district policy, and administrative regulations.
4. Students are not permitted to use district technology to search the Internet for non-educational purposes. This includes "free search/surf" the Internet which is defined as unsupervised searching of the Internet without an educational teacher-approved purpose.
5. A user must not knowingly attempt to access educationally inappropriate material. If a user accidentally reaches such material, the user must **immediately** back out of the area on the Internet containing educationally inappropriate material. The user must then notify the teacher or campus/building administrator of the site address that should be added to the filtering software, so that it can be removed from accessibility.

Publishing on the Internet:**Recognition:**

First and last names and grade level may be used on the Internet to recognize personal achievements.

Permission for the following items is granted or denied through the initial Emergency Information and Medical/Parent Authorization form given to each student at the beginning of the school year.

Student Work:

Student work will only be published on the Internet with parental permission. Examples of published work could include short stories, poems, slide shows, and/or artwork. First and/or last names may be included with the student work.

Photographs:

Student photographs will only be published on the Internet with parental permission. First and/or last names may be included with the photograph.

Exceptions to the above:

Any exceptions to the items above will be secured through the Communication Office. Individual campuses may elect not to publish student work and/or photographs on the campus website even though the parent has given permission to do so.

Web Authoring:

The district and each campus have an authorized web site. Students, district employees, and community members are strictly prohibited from authoring a private web site which represents itself as the official site for the district. For example, this would include, but not be limited to, campus, club, and department sites.

Network Etiquette:

Students are not provided e-mail accounts and are prohibited from accessing e-mail services while using district equipment. System users of e-mail or other communication messaging systems are expected to observe the following network etiquette. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited. Transmitting obscene messages or pictures is prohibited. Revealing personal addresses or phone numbers of the user or others is prohibited. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Inappropriate Use:

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations below, that violate the rules of network etiquette, or that hamper the integrity or security of this or any networks connected to the Network/Internet. Please refer to the "Consequences of Violation" section of this document.

Commercial Use: Use for commercial purposes, income-generating or "for-profit" activities, product advertisement, or political lobbying is prohibited. Sending unsolicited junk mail, or chain letters, is prohibited.

Vandalism/Mischief: Vandalism and mischief are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Network/Internet, or any networks that are connected to the Network/Internet. This includes, but is not limited to, the creation or propagation of computer viruses. Any interference with the work of other users, with or without malicious intent, is construed as mischief and is strictly prohibited.

Playing Games and Downloading Music or Video Files or Game Files: These activities are strongly prohibited. The district has access to subscription-based resources for instructional purposes for students and district employees.

Electronic Mail Violations: Forgery of electronic mail messages is prohibited. Reading, deleting, copying, or modifying the electronic mail of other users, without their permission, is prohibited.

File/Data Violations: Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission, is strictly prohibited.

System Interference/Alteration: Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Unauthorized Disclosure: Unauthorized disclosure, use and dissemination of personal information regarding students and employees are prohibited.

Security:

Reporting Security Problems:

If a user identifies or has knowledge of a security problem on the Network/Internet, such as filtering software not working, the user should immediately notify a teacher, administrator or the System Administrator. The security problem should not be shared with others.

Impersonation:

Attempts to log on to the Network/Internet impersonating a system administrator or district employee may result in revocation of the user's access to Network/Internet.

Other Security Risks:

Any user identified as having had access privileges revoked or denied on another computer system may be denied access to the district's Network/Internet.

Violations of Law:

Transmission of any material in violation of any US or state law is prohibited. This includes, but is not limited to: copyrighted material, threatening, harassing, or obscene material; or material protected by trade secret. Any attempt to break the law through the use of a district Network/Internet account may result in litigation against the offender by the proper authorities. If such an event should occur, the district will fully comply with the authorities to provide any information necessary for the litigation process.

Consequences of Violations:

Any attempt to violate the provisions of these guidelines may result in revocation of the user's access to the Network/Internet, regardless of the success or failure of the attempt. In addition, disciplinary action consistent with the district discipline policy and/or appropriate legal action, which may include restitution, may be taken. District administrators will make the final determination as to what constitutes inappropriate use. With just cause, the System Administrator or other administrator, may deny, revoke, or suspend Network/Internet access as required, pending the outcome of an investigation.

Computer Software Policy

In accordance with Board Policy EFE (local) and Administrative Regulation EFE-R, it is the practice of the district to respect all computer software copyrights and to adhere to the terms of all software licenses to which the district is a party. Technology Services is charged with the responsibility of enforcing these guidelines.

All computer software installed on district equipment must be purchased, reported to, and installed by Technology Services (or its designee). Software acquisition channels are restricted to ensure that the school district has a complete record of all software that has been purchased for district computers and can register, support, and upgrade such software accordingly. Software on district computers used for instructional and/or administrative purposes must be approved by a district curriculum coordinator and Technology Services.

Students, district employees, and volunteers may not duplicate any licensed software or related documentation for use either on the district's premises or elsewhere unless Technology Services is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject

the employee and/or the school district to both civil and criminal penalties under the United States Copyright Act.

Students, district employees, and volunteers may not give software to any third party including relatives, clients, contractors, etc. District employees, students, and volunteers may use district-approved software on local area networks or on multiple machines only in accordance with applicable license agreements.

For further information regarding the purchase and installation of computer software, please call the district's HELP Desk at 281.897.HELP (4357).

DISCLAIMER:

These guidelines apply to stand-alone computers as well as computers connected to the Network/Internet. The district makes no warranties of any kind, whether 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, mis-deliveries, or service interruptions caused by its negligence or user errors or omissions. The district is not responsible for phone/credit card bills or any other charges incurred by users. Use of any information obtained via the Network/Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services. 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 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 electronic communications system.