Jim Hogg County ISD

Children's Internet Protection Act

CIPA Compliance

Contents

Jim Hogg County ISD

Children's Internet Protection Act

CIPA Compliance

The **JIM HOGG COUNTY ISD** (District) believes that technology and its utilization enhances the quality and delivery of education and is an important part of preparing children for life in the 21st century. The community of technology users must understand that the Internet is a global, fluid community, which remains largely unregulated. While it is an extremely valuable educational tool, there are sections that are not commensurate with community, school, or family standards. The District believes that the Internet's advantages far outweigh its disadvantages and will provide an Internet filtering device which shall be used to block or filter access to inappropriate information and material on the Internet, in electronic mail or other forms of electronic communications. It should not be assumed that users are completely prevented from accessing inappropriate materials or from sending or receiving objectionable communications.

It is the policy of the **JIM HOGG COUNTY ISD** to:

1. prevent user access over its computer network to, or transmission of inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;
3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors;
4. educate minors about appropriate online behavior, including interacting with other individuals on social networks, websites, and in chat rooms and cyber bullying awareness and response; and
5. comply with the Children's Internet Protection Act, the Neighborhood Children's Protection Act and the Protecting Children in the 21st Century Act (collectively "**CIPA**").

Additionally, the District considers access to the Internet and computer resources a privilege, not a right. Therefore, users violating the District's Administrative Rules—Code of Conduct and User agreement—may be subject to revocation of these privileges and potential disciplinary and and/or civil and criminal action.

RULES:
A. GENERAL PROVISIONS:

1. CIPA COMPLIANCE:

The District will have the following in continuous operation, with respect to all computers belonging to the District:

(a) A qualifying "technology protection measure," as that term is defined in **CIPA,** to block or filter access to the Internet by adults and minors to visual depictions that are obscene, pornographic or harmful to minors as those terms are defined in **CIPA**. Subject to staff supervision and advance approval by a technology administrator or other person authorized by the District, the technology protection measure may be disabled for adults engaged in bona fide research or other lawful purposes.

(b) Procedures, materials and/or guidelines developed by the Curriculum and Instruction Division and the Technology Services Division which provide for monitoring the online activities of users

and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are obscene, pornographic, or harmful to minors, as those terms are defined in **CIPA**, and to material deemed inappropriate for minors as determined by the District. Such procedures, materials or guidelines will be designed to:

1. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to harmful or inappropriate matter on the Internet and the World Wide Web;
2. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;
4. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

Restrict minors' access to materials "harmful to minors," as that term is defined in **CIPA**.

(c) Educational materials, guidelines and procedures which shall be used to educate minors on appropriate online behavior, including without limitation interacting with other individuals on social networking Web Sites and chat rooms and cyberbullying awareness and response.

2. Education, Safety and Security of Minors:

Teachers and others working with students will, in accordance with District guidelines, educate minors on appropriate online behavior, including without limitation interacting with other individuals on social networking Web Sites and chat rooms and cyberbullying awareness and response and caution students that they should:

(a) Never place personal contact information or a personal photograph on the Internet, e-mail or any on-line communication device. Personal contact information includes full name, address, telephone number, school address, or names of family or friends.

(b) Never arrange a face-to-face meeting with someone you meet online.

(c) Never open attachments or files from unknown senders.

(d) Always report to a teacher any inappropriate sites you observe being accessed by another user or that you access accidentally.

3. Internet Searches:

Students should be supervised by instructional personnel when accessing network and internet resources and the following guidelines apply:

Elementary School:

(a) Elementary school students may visit sites a teacher has pre-selected for them. Searches should be completed with child friendly Internet search engines (for instance see: www.nettrekker.com)

Middle School/High School:

(b) Middle school and high school students may visit sites a teacher has pre-selected for them. They may use search engines other than child-friendly search engines when directed to do so by their teacher.

(c) Non-instructional personnel, such as After School Program (ASP) workers, are not permitted to allow students to access technology resources unless it is an instructional activity.

4. Network Security:

Maintaining network security is the responsibility of all users. Users should:

(a) Not leave an unsecured workstation without logging out of the network;

(b) Not share or disclose passwords; and

(c) Notify appropriate personnel immediately if a potential security problem is identified.

5. Acceptable Use Agreement:

Prior to receiving access to the District's technology resources, employees and students should complete an Acceptable Use Agreement indicating they accept and agree to the provisions of **Administrative Rule(Use of Technology Resources in Instruction and Internet Safety Policy)**.

6. Copyright:

(a) Students and employees should comply with Administrative Rule EGAD (Intellectual Property), as well as federal, state or local laws governing copyrighted material.

(b) Students/employees will not: (1) Download or upload files to the District's technology that might cause copyright infringement; or

(c) Install, use, store, distribute or transmit unauthorized copyrighted or trademarked materials on District technology.

7. The Principal:

If students or employees believe that the implementation of this Rule denies access to material that is not prohibited by this Rule, he/she should submit that concern in writing to the school principal or designee or his/her supervisor or designee. The principal, supervisor or designee should report this concern to the appropriate District office within ten (10) school days.

B. AUTHORITY:

1. The District:

The District provides its students and authorized employees with access to and use of its technology consistent with the District's vision and strategic goals. Therefore, the District reserves the right to monitor, access, and disclose the contents of any user's files, activities, or communications to any appropriate authority, including law enforcement.

2. Employees:

Principals and Administrators will endeavor to inform students and employees of the responsibilities associated with use of the District's technology. To this end, Administrative Rule IJNDB (Use of

Technology Resources in Instruction and Internet Safety Policy) is included in the Parent Information Guide. Any attempts to harm, modify, destroy or otherwise change the District's data and technology should be reported to appropriate District authorities. Staff will refer to District Administrative Rules governing employee and student conduct, including,(Student Conduct: Codes of Conduct), when addressing inappropriate use or abuse of District technology privileges.

3. Students:

Students will adhere to all policies, Rules and regulations issued by the District and their respective school.

C. PROHIBITED USES:

Students and employees who violate District/school policies, Rules or regulations governing the use of the District's technology and network resources may have their network privileges suspended or revoked and will be subject to District Administrative Rules applying to employee and student conduct including, for students, the provisions of the appropriate District Code of Conduct Ethical use of District technology prohibits the following activities by all users:

1. Accessing, sending, creating or posting material or communication that is:
    a. Damaging;
    b. Abusive;
    c. Obscene, lewd, profane, offensive, indecent, sexually explicit, or pornographic;
    d. Threatening or demeaning to another person—CYBERBULLYING—; or
    e. Contrary to the District's Rules on harassment and/or bullying.
2. Posting anonymous or forging electronic communications.
3. Using the network for financial gain, advertising or political lobbying to include student elections.
4. Engaging in any activity that wastes, monopolizes, or compromises the District/school's technology or other resources.
5. Illegal activity, including but not limited to copying or downloading copyrighted software, music or images, or violations of copyright laws.
6. Using the District network for downloading music or video files or any other files that are not for an educational purpose or, for students, a teacher-directed assignment.
7. Attempting to gain unauthorized access to District/school technology resources whether on or off school property.
8. Using non-educational Internet games, whether individual or multi-user.
9. Participate in any on-line communication that is not for educational purposes or, for students that are not specifically assigned by a teacher.
10. Using voice over IP, internet telephony, video and/or audio communication devices without teacher supervision.

11. Using District/school technology resources to gain unauthorized access to another computer system whether on or off school property (e.g. "hacking").
12. Attempting to or disrupting District/school technology resources by destroying, altering, or otherwise modifying technology, including but not limited to, files, data, passwords, creating or spreading computer viruses, worms, or Trojan horses; engaging in DOS attacks; or participating in other disruptive activities.
13. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.
14. Attempting/threatening to damage, destroy, vandalize, or steal private/school property while using school technology resources.
15. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.
16. Using or attempting to use the password or account of another person, utilizing a computer while logged on under another user's account, or any attempt to gain unauthorized access to accounts on the network.
17. Connecting to or installing any personal technology computing device or software without prior approval of the District's Technology Services Division.
18. Attempting to obtain access to restricted sites, servers, files, databases, etc.
19. Exploring the configuration of the computer operating system or network, running programs not on the menu, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations.
20. Leaving an unsecured workstation without logging out of the network.

D. E-MAIL:

E-mail accounts are provided to employees for professional purposes (see Administrative Rule GBDA [Communications System: District's Inter and Intra Communications]). Students may not access their personal e-mail accounts. Where used in the following guidelines, User/Users refers to both employees and students:

1. Persons outside the District may be able to receive information regarding an employee's communications and use of the network from the District.
2. Employees should request permission from the appropriate administrator prior to sending an e-mail message to an entire school staff or District level division.
3. Employee use of e-mail to transmit confidential student information, as defined in Administrative Rule JRA (Student Records), or sensitive personnel information is prohibited, except where the confidential information is sent in an e-mail directly to a parent/guardian, the subject of the e-mail, or a school official.

4. When an employee sends e-mail that contains confidential information, the employee should refer to the subject of the e-mail by first name only and should include the following disclaimer:
5. "This e-mail may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any unauthorized dissemination, distribution or copying of any information from this e-mail is strictly prohibited. If you receive this e-mail in error, please notify us immediately by collect telephone call at (telephone number) or electronic mail (email)."
6. The District reserves the right to monitor whatever a User does on the network and to make sure the network functions properly.
7. A User has no privacy as to his/her communications or the uses he/she makes of the Internet.
8. Users should not use e-mail for personal gain or personal business activities.
9. Users will not use e-mail to distribute inappropriate material through pictures, text, forwards, attachments, and other forms of information.
10. Users will not send anonymous e-mail, nor will they harass others through e-mail.

E. WEB SITE PUBLISHING:

1. Publication of student information, work and pictures is governed by Administrative Rule CFIA (Monitoring-Recording Staff and Students).
2. Web pages or blogs hosted on or linked from Jim Hogg County ISD Web server will not:
    a. Include any information that indicates the physical location of a student at a given time, other than attendance at a particular school or participation in school activities where appropriate consent has been received.
    b. Display personal information, photographs, videos, streaming video, or audio clips of any identifiable student without a prior written permission slip Permission to Display Student Photograph if a parent/guardian has "opted out" of the release of directory information as stated in the Directory Information Statement in the Parent Information Guide.
3. Prior to placing a student's material on the Internet, the student should sign Permission to Display Student Work. For students under the age of 18, the permission slip should also be signed by the student's parent/guardian.
4. Students may retain the copyright on the material they create that is subsequently displayed or performed on the District's Web site or individual school Web pages or blogs.

F. EMPLOYEE CREATED WEB PAGES AND/OR BLOGS:

The District assumes no responsibility for schools or individual employees who do not comply with the following provisions:

1. Employees may create or link to individual Web pages and/or blogs on an external site provided these external sites meet the District's definition of "educational purposes" as stated in Section G below. Any links to external sites that fail to meet that definition will be removed.
2. Each employee will be responsible for maintaining his/her Web pages or blogs in cooperation with the school Web Publisher. Specifically, all material originating from the employee and placed on the employee Web pages/blogs will be consistent with the Web Page Publishing and Compliance Guidelines and approved through the compliance process established by the District Web Publisher (Web Master).
3. The District Web site and individual employee Web pages/blogs will not: a. Contain public message boards or chat-room areas. However, employees may allow two-way communication on blogs or private message boards as a part of the classroom curriculum as long as the employee previews (moderates) and approves all blog comments before they are posted on the Internet.

    c. Allow the display of unsolicited comments from the general public. Any solicited public feedback should be reviewed by the employee before posting. Any questionable or inappropriate content will immediately be removed by the employee, the School Web Publisher or by the District Web Publisher (Web Master) with no notification.

G. DEFINITIONS:

As used in this Rule, the terms and definitions contained in **CIPA** are expressly incorporated herein by reference and the following additional definitions shall also apply:

1) "**Blogs**" (short for Web Logs) means dynamic web sites consisting of regularly updated entries displayed in reverse chronological order. They read like a diary or journal, but with the most recent entry at the top. Blogs can allow for open comments meaning other individuals can respond to a posted entry. Open comments is an optional feature for most blog Web sites.
2) "**Chat Rooms**" means a Web site, part of a Web site, or part of an online service, that provides a venue for communities of users with a common interest to communicate in real time.
3) "**Cookies**" means messages that may include personally identifiable information, which are stored in a text file and used to identify visitors and possibly prepare customized Web pages for them.
4) **"Cyberbullying"** means bullying through an electronic medium such as a computer or cell phone.
5) "**DoS attack**" means a denial-of-service attack designed to overload an electronic network with useless traffic and messages.
6) "**Educational purposes**" means it relates to curriculum and instruction, research, career or professional development, or administrative purposes.
7) "**E-mail**" means an electronic message generated using the District's e-mail and/or Web based email. It is also used generically to mean either the District's e-mail system or a Web-based e-mail system.
8) "**External site**" means Web sites and materials not hosted on the District's Web server.

9) "**Hacking**" means the illegal activity of breaking into a computer system or electronic network, regardless of intent to cause harm.
10) "**Inappropriate material**" means material that does not serve an instructional or educational purpose and that includes, but is not limited, to material that:
    (i) is profane, vulgar, lewd, obscene, offensive, indecent, sexually explicit, or
    (ii) threatening;
    (iii) advocates illegal or dangerous acts;
    (iv) causes disruption to Jim Hogg County ISD, its employees or students;
    (v) advocates violence; or
    (vi) contains knowingly false, recklessly false, or defamatory information.
11) "**Instructional activity**" means a classroom activity that focuses on appropriate and specific learning goals and objectives.
12) "**Message board**" means a virtual bulletin board, where people post and view messages.
13) "**Mirroring**" means the creation of other Web sites that replicate or duplicate an existing Web site in order to reduce network traffic or improve performance and availability of the original Web site.
14) **"Social networking"** means the use of Web sites or other online technologies to communicate with people and share information, resources, etc.
15) "**Teacher directed**" means that the teacher gives to the students' specific instructions for activities and assignments.
16) "**Teacher supervised**" means that a staff member will oversee the activities of the students.
17) "**Technology**" means but is not limited to electronic media systems such as computers, computing devices, peripheral devices, telecommunication equipment, electronic networks, messaging, and Web site publishing, and the associated hardware and software programs used for purposes such as, but not limited to, developing, retrieving, storing, disseminating, and accessing instructional, educational, and administrative information.
18) "**Trojan Horse**" means a destructive computer program that enters onto a computer by pretending to be a simple and safe computer application.
19) "**Users**" means District students, certain employees, including school and Central Office staff, and other authorized persons who use the District's technology.
20) "**Virus**" means a replicating computer program or piece of code that is loaded onto a computer without the user's knowledge and may attach itself to other computer programs and spread to other computers.
21) "**Web Bug**" means an invisible image placed on a Web page that is embedded in JavaScript code that collects information about a user's Internet behavior.
22) "**Web Page**" means a single document or file on the Web, identified by a unique URL.
23) "**Web Site**" means a collection of "pages" or files on the Web that are linked together and maintained by a company, organization, or individual.
24) "**Worms**" means a type of virus that can replicate itself and use a computer's memory but can or cannot attach to other computer programs.