



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

A. Educational Purpose

1. The district's Network/Internet system has a limited educational purpose.
 - a. The term "educational purpose" includes use of the system for classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.
 - b. Students and staff may not use the system for personal commercial purposes, including offering or purchasing products or services.
 - c. Users may not use the system for lobbying activities, as defined under Education Code section 7054. This provision shall not limit the use of the system by students or staff for the purposes of communicating with elected representatives or expressing views on political issues.
 - d. Staff may use the district Network/Internet system for communications related to collective bargaining and union organizational activities, with reasonable frequency, which do not interfere with educational activities. Concerted activities and work stoppage related activities will not be permitted.

B. Discipline for Violation of Policy

1. The District will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the District Network/Internet system. This may include release of district loaned equipment to law enforcement.
2. User access to the District Network/Internet system will require the use of an account name and password to enable individual users to be identified. Elementary students may use the Internet through a classroom user account and password.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- 3. In the event there is an allegation that a student has violated this policy, the student discipline will be conducted in the manner set forth in the student disciplinary policies and regulations.
- 4. Employee violations of this policy will be handled in accord with District policy and the collective bargaining agreement.
- 5. Any files, electronic mail and other information on the District's networks or equipment is subject to search at any time.

C. Promoting the Effective Educational Use of the Internet

- 1. The district will provide professional development opportunities for teachers in the effective use of the Internet for instructional purposes.
- 2. All sites linked to through the District web sites should be prescreened to ensure such sites are appropriate in light of the age of the student and relevant to the course objectives.
- 3. The district and teachers will seek to limit student exposure to commercial advertising and product promotion, especially advertising or promotion of youth-oriented products and services, in the development of the district or classroom web sites or other assignments utilizing the Internet.
- 4. For students at the elementary school level, access to information on the web will generally be limited to access of prescreened sites and must be closely supervised by the teacher.
- 5. For students at the secondary school level, students may access sites that are not prescreened, in a manner prescribed by their school.

D. Protections Against Access to Inappropriate Material

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	--



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

1. Inappropriate material.
 - a. The District has identified the following types of material as Prohibited, Restricted, and Limited Access Material.
 - i. Prohibited Material. Prohibited Material may not be accessed by the students or staff at any time, for any purpose. This material includes material that is obscene, child pornography, material that is considered harmful to minors, as defined by the Children's Internet Protection Act. The district designated the following types of materials as Prohibited: Obscene materials, child pornography, material that appeals to a prurient or unhealthy interest in, or depicts or describes in a patently offensive way, violence, nudity, sex, death, or bodily functions, material that has been designated as for "adults" only, and material that promotes or advocates illegal activities.
 - ii. Restricted Material. Material that is Restricted may not be accessed by elementary students at any time for any purpose. Restricted Material may be accessed by junior high or high school students in the context of specific learning activities that have been approved by teachers or by staff for legitimate research or professional development purposes. Materials that may arguably fall within the description provided for Prohibited Material that have clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be Restricted. In addition, Restricted Material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are Restricted unless such sites have been specifically approved by the school.
 - iii. Limited Access Material. Limited Access Material is material that is generally considered to be non-educational or entertainment. Limited Access Material may be accessed in the context of specific learning activities that are directed by a teacher. Limited Access Material includes

REFERENCE	REVISED:
California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)	12/11/97 6/21/01 5/16/02



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investments.

- b. If a user inadvertently accesses material that is considered Prohibited or Restricted, he/she should immediately disclose the inadvertent access in a manner specified by their school. This will protect the user against an allegation that they have intentionally violated the policy.
- c. The determination of whether material is Prohibited, Restricted, or Non-educational shall be based on the content of the material and the intended use of the material, not on the protective actions of the Technology Protection Measure. The fact that the Technology Protection Measure has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the Technology Protection Measure has protected access to certain material shall not create the presumption that the material is inappropriate for users to access.

2. Technology Protection Measure.

- a. The District has selected a Technology Protection Measure for use with the District Internet system and has specified the manner in which the Technology Protection measure will be configured. The Technology Protection Measure will always be configured to protect against access to material that is obscene, child pornography, and material that is harmful to minors, as defined by the Children's Online Protection Act. The district or individual schools may, from time to time, reconfigure the Technology Protection Measure to best meet the educational needs of the district or schools and address the safety needs of the students.
- b. The Technology Protection Measure may not be disabled at any time that students may be using the district Internet system, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The Technology Protection Measure may be disabled during non-student-use time for system administrative purposes.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	--



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- c. Technology Protection Measures have been found to inappropriately block access to appropriate material. To ensure that the implementation of the Technology Protection Measure is accomplished in a manner that retains District control over decision-making regarding the appropriateness of material for students, does not unduly restrict the educational use of the District Internet system by teachers or students, and ensures the protection of students' constitutional rights of access to information and ideas, authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the Technology Protection Measure.
 - i. Authority to temporarily unblock access will be granted to the site administrators and/or his/her designee(s). Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are necessary to ensure the security of the system. The Director of Technological Support shall determine such standards.
 - ii. To temporarily unblock a site, the authorized individual must review the contents of the site, outside of the presence of any student, prior to allowing access to the site by a student.
 - iii. Reports of all instances of temporary unblocking will automatically be forwarded to the Director of Technological Support.
 - iv. If an authorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forwarded to the Director of Technological Support. The Director of Technological Support may make a decision to permanently unblock access to the site or may delegate the decision to the District Technology Advisory Committee. A list of all sites that have been permanently unblocked, together with the rationale for making the decision to unblock the site, will be forwarded on a monthly basis to the Superintendent, the Technology Protection Measure company, and the District Technology Advisory Committee..

E. Supervision, Monitoring, Search and Seizure, and Retention of Records

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

1. Student use of the district Internet system will be supervised by staff in a manner that is appropriate to the age of the students and circumstances of use. The building administrator, or his/her designee, will develop and disseminate staff supervision requirements for their respective schools. Computers used by students in classrooms and labs will be positioned to facilitate effective staff supervision.
2. The district will monitor use of the Internet through a regular analysis of Internet usage. Individual schools may implement any additional monitoring systems desired.
3. Users have no privacy expectations in the contents of their personal files and records of their online activity while on the district system.
4. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating district policy, regulations, or the law. An individual search may be conducted at District discretion. Individual search of user's e-mail will first be approved by a district administrator responsible for supervision of the student or staff or by the superintendent or his/her designee. Students and staff have no expectation of privacy from review of any information contained in District owned equipment at any time.
5. The superintendent, or his/her designee, will implement an Internet records retention system that is in accord with state law. Internet records that are not subject to retention will be destroyed on a regular basis.

F. Safety and Security of Students When Using Direct Electronic Communication

1. The district will provide e-mail access for students and staff.
 - a. Elementary and secondary students may use e-mail through classroom accounts or accounts where the teacher has full access to all communication. Secondary students may request a time limited e-mail account to serve a specific educational purpose. Student accounts will be established with a username that will protect the personal identity of the student.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	--



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- b. Staff will be provided with individual accounts. Staff will use a signature file that identifies who they are and their position with the district.
 - c. Students may not establish or access web-based e-mail accounts on commercial services through the district Internet system unless such accounts have been approved for use by the individual school.
 - d. Excessive use of e-mail by a student may raise a reasonable suspicion that the student is using electronic mail in violation of this policy.
2. Students may use real-time electronic communication, such as chat, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the district or individual school.

G. Illegal, Unauthorized, and Inappropriate Activities

- 1. Illegal Activities
 - a. Users will not attempt to gain unauthorized access to the District Network/Internet system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files.
 - b. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.
 - c. Users will not use the District Network/Internet system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

2. Inappropriate Language

- a. Restrictions against Inappropriate Language apply to all speech communicated through the district Internet system, including but not limited to public messages, private messages, and material posted on web pages.
- b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- c. Users will not post information that, if acted upon, could cause damage or a danger of disruption.
- d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
- f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

3. Plagiarism and Copyright Infringement

- a. Users will not plagiarize works that they find on the Internet.
- b. Users will respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to the Internet.

H. System Security and Resource Limits

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

1. System Security

- a. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account, including protecting the privacy of their password.
- b. Users will immediately notify the system administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- c. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures.

2. Resource Limits.

- a. Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer or diskette.
- b. Users will not misuse district, school, or personal distribution lists or discussion groups for sending irrelevant messages. Irrelevant messages include cartoons, chain letters, hoaxes, virus warnings, and funny or inspirational messages forwarded to users.
- c. Users will check their e-mail frequently, at least once a week, delete unwanted messages promptly, and stay within their e-mail quota.
- d. Users will subscribe only to approved high quality discussion groups that are relevant to their education or professional/career development.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- e. Excessive use of the district Internet system may raise a reasonable suspicion that the student is using the system in violation of district policy and regulations.

I. Protection of Student Confidentiality and Privacy

1. All contracts with third party providers of data management services for the district will be reviewed to ensure compliance with federal and state student privacy and records retention laws.
2. Staff transmission of student confidential information via e-mail must be in compliance with all federal and state student privacy laws.
 - a. The "subject line" of the e-mail should provide an indication that the e-mail contains confidential student information.
 - b. A hard copy of any e-mail containing student confidential information will be retained in accord with District student records retention requirements.
3. Teachers will ensure the protection of student personal information when establishing any relationship with a third-party site or system.
 - a. Teachers may require, encourage, or allow students to provide established individual accounts on a third party site or system only under the following circumstances:
 - i. The establishment of the account is necessary to achieve identified educational purpose.
 - ii. There is no commercial advertising for youth interest products or services on the third party system.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- iii. Student personal information and student use data will not be collected, analyzed and/or used for commercial advertising or marketing purposes.
 - iv. A minimum amount of non-identifying information is collected for the purpose of establishing the account.
 - v. The third party system has committed to maintain the privacy of any information provided.
 - vi. The third party system provides a process by which a parent may access, review, and remove their child's account information.
- b. Signed parental permission must be obtained prior to the establishment of the student account. Notice to the parent about proposed student accounts on third party systems must include the following information:
- i. The name, URL, and privacy policy of the third party system.
 - ii. Description of the educational purpose for the establishment of the account.
 - iii. The period of time for which the account will be established.
 - iv. Information on how they can access their child's records on the third party site.
2. Privacy and Communication Safety Standards. Students and staff will abide by the following privacy and communication safety standards when using the district Internet system, including use of electronic communications and the web.
- a. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent's name, home address or location, work address or location, or phone number.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- b. It is impermissible to disclose the full name or any other personal contact information of elementary and junior high school students, except with principal approval to education institutions for educational purposes, or except with superintendent approval.
 - c. It is impermissible to disclose personal contact information for high school students, except to education institutions for educational purposes, companies or other entities for career or college development purposes, or with specific superintendent approval.
 - d. Students will not forward a message that was sent to them privately without permission of the person who sent them the message.
 - e. Students will not agree to meet with someone they have met online without their parent's approval and participation.
 - f. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.
4. The following provisions address the disclosure of student information, posting student-created material, and posting pictures of students on the District web site. Parents must approve such disclosure and posting.
- a. For students, the following standards apply: Students will use a limited student identification (first name and last initial or other school-developed identifier). Group pictures without identification of individual students are permitted. Student work may be posted with the limited student identification. All student posted work will contain the student's copyright notice using the limited student identification.

J. Copyright Management

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

1. The district will respect the copyright rights of students and staff.
 - a. Students own the copyright to their creative works, including works created using district resources. The Internet agreement signed by parents will include a request for permission from parents to post student work on the Internet. All student work posted on the Internet will contain a copyright notice indicating the ownership of that work by the student(s).
 - b. District Staff own the copyright to works created outside of the scope of their employment responsibilities and without the use of district resources. District staff may post such work on the district web site to facilitate access by students and/or staff. Notice of such posting and claim of ownership must be provided to the Superintendent. By posting such work to the district's web site, the staff member will grant a non-exclusive license or permission for any staff or student within the district to freely use such work.
 - c. The district shall own the copyright on any works created by district staff within the scope of their employment responsibilities.
2. The district will promote respect for the copyright rights of others.
 - a. The district will provide instruction to staff and students on their rights and responsibilities with respect to the copyright ownership rights of others.
 - b. No material may be disseminated through the district Internet system or posted on the district Internet site unless that material is original, in the public domain, used in accord with the fair use provisions of the copyright law, or is disseminated or posted with permission of the copyright owner.

K. District Web Site Regulations

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

1. District Web Site.
 - a. The district will establish a district web site. Material appropriate for placement of the district web site includes: District information, school information, teacher or class information, student projects, and student extracurricular organization information. Personal, non-educationally-related information will not be allowed on the district web site.
 - b. The Superintendent will designate a district web publisher, responsible for maintaining the official district web site and monitoring all district web activity. The web publisher will develop style and content guidelines for official district and school web materials and develop procedures for the placement and removal of such material. All official district material originating from the district posted on the district web site must be approved through a process established by the district web publisher.
2. School Web Pages. The site principal will designate a school web publisher, responsible for managing the school web site and monitoring class, teacher, student, and extracurricular web pages. All official material originating from the school will be consistent with the district style and content guidelines and approved through a process established by the school web publisher. The school web publisher will develop additional guidelines and placement processes for the school web site. All other web pages shall be a closed forum. There shall be complete school control of all posted web information.
3. Teacher or Classroom Web Pages. Teachers may establish web pages for use with class activities or that provide a resource for other teachers. Teachers will be responsible for maintaining their class or educational resource sites. Teacher web pages will be developed in such a manner as to reflect well upon the district and school.
4. Student Web Pages.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---



SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

- a. Students may create a web site as part of a class activity. Material presented on a student class activity web page must meet the educational objectives of the class activity. Such pages shall be strictly limited to the educational objectives and subject to the individual limitations of the school for that activity.
- b. It will not be considered a violation of a student's right to free speech to require removal of material that fails to meet established educational objectives or that is in violation of a provision of the Student Internet Use Policy or student discipline policies and regulations. Student web pages must include the following notice: "This is a student web page. Opinions expressed on this page shall not be attributed to the district." The District reserves the right to remove any student web sites from the network at any time.

5. Web Page Requirements

- a. All Internet Use Policy provisions, including those addressing inappropriate language, privacy, and copyright, will govern material placed on the district web site. Disciplinary policies and regulations will also govern such material.
- b. Web pages shall not contain the identification information or pictures of the student or student work unless such provision has been approved by the student's parents/guardians.
- c. Material placed on the web site is expected to meet academic standards of proper spelling, grammar, and accuracy of information.
- d. All web pages will carry a stamp indicating when it was last updated and the e-mail address of the person responsible for the page.
- e. All web pages should have a link at the bottom of the page that will help users find their way to the appropriate home page.

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p style="text-align: center;">REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	--



ARTICLE III EDUCATIONAL PROGRAM

SECTION 3.2 CURRICULUM AND INSTRUCTION

Sec. 3.2-9 District Network/Internet Safe and Responsible Use Procedure

f. Users should retain a back-up copy of their web pages.

6. Web Site Concerns

a. The district web site and each School web page will have a "Web Site Concerns" link. This link will take the reader to a page that provides the following information:

Davis Joint Unified School District seeks to ensure that all materials placed on the district or school web sites are placed in accord with copyright law and do not infringe on the rights of or harm others in any way. To accomplish this we are taking three steps:

- We have provisions in our Internet Use Policy that address copyright, defamation, harassment, invasion of privacy, and other harmful speech. <link to policy>
- We have established web site management procedures to review materials prior to their placement on the web site. <link to procedures>
- We will promptly respond to any issues of concern . If you have a concern about material placed on our web site, please contact us. <link to e-mail to an administrator who has the responsibility of promptly responding to any complaint>

<p style="text-align: center;">REFERENCE</p> <p>California Department of Education's Acceptable Use Policy Guidelines Child Internet Protection Act (CIPA)</p>	<p>REVISED:</p> <p>12/11/97 6/21/01 5/16/02</p>
---	---