

1. The District is providing Internet access to its employees, board members, and students. The District's Internet system has a limited educational purpose as defined in the administrative regulation. The District's Internet system has not been established as a public access service or a public forum. The District has the right to place restrictions on use to ensure that use of the system is in accord with its limited educational purpose.
2. Student use of the District's Internet system will be governed by this policy, related District and school regulations, and the student disciplinary code. Teachers/staff use will be governed by this policy, related District and school regulations, District employment policy, and the collective bargaining agreements. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the District Internet system. Users have no privacy expectations in the contents of their personal files and records of their online activity while on the District system.
3. By this policy, the District restricts access to materials and places restrictions on student speech through use of the Internet for educational and business reasons. The District declares its ownership of the relevant hardware and software and asserts its right to review and exercise its ownership at any time by search of the system and its equipment, and any information on it. Use of the Internet by students and teachers/staff shall be subject to monitoring and search, and teachers/staff and students should take notice that they have no expectation of privacy in any information contained on District owned equipment.
4. The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District Internet system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data, interruptions of service, or exposure to inappropriate material or people. The District is not responsible for the accuracy or quality of the information obtained through the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system. Users or parents/guardians of users will indemnify and hold the District harmless from any losses sustained as the result of misuse of the system by user. Use of the system by students will be limited to those students whose parents/guardians have signed a Technology Use Support Agreement.
5. The District has developed and approved this policy in accord with the statutory requirements of the Children's Internet Protection Act. The policy was developed with input and feedback from teachers/staff, parents/guardians, and community members. The policy represents the District's good faith efforts to promote the safe, ethical, responsible, and legal use of the Internet, support the effective use of the Internet for educational purposes, protect students against potential dangers in their use of the Internet, and ensure accountability.
 - a. The District will promote the effective, educational use of the Internet in schools through professional development and the establishment of a District web site that will provide access to prescreened, appropriate, educationally relevant material.

- b. Student and teachers/staff users of the District's Internet system will receive instruction regarding the safe, ethical, legal, and responsible use of the Internet and of the District's Internet system and their rights and responsibilities under this policy.
- c. Student use and activities will be structured in a manner that is appropriate to the age and skills of students, recognizing the importance of providing more secure environments for younger students and supporting safe, responsible, independent use by older students.
- d. The District will protect against access to materials that are considered inappropriate for users to access through the District Internet system in the following manner:
 - i. The District regulations will designate certain categories of materials as Prohibited, Restricted, or Limited Access Material. Prohibited Material may not be accessed by the students or teachers/staff at any time, for any purpose. Restricted Material may not be accessed by elementary students, but may be accessed by junior high school students or high school students in the context of specific learning activities that have been approved by a teacher or by teachers/staff for professional development purposes. 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.
 - ii. The District will implement the use of a Technology Protection Measure, which is a specific technology that will protect against access to visual depictions that are obscene, child pornography, and materials that are harmful to minors, as defined by the Children's Internet Protection Act. At the discretion of the District or school, the Technology Protection Measure may also be configured to protect against access to other material considered inappropriate for students to access.
 - iii. 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. Authorized teachers/staff at the District Office or school sites may temporarily unblock access to sites containing appropriate material, if access to such sites has been inappropriately blocked by the Technology Protection Measure. Permanent unblocking of websites will be decided by a committee consisting of members of the Instructional Services Division.
 - iv. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the Technology Protection Measure.
- e. Student use of the District Internet system will be supervised by teachers/staff in a manner that is appropriate to the age of the students and circumstances of use.
- f. The District will develop procedures to monitor student use of the Internet through an analysis of Internet usage records.
- g. The District and schools will establish regulations and procedures to protect the safety and security of students when using direct electronic communications.

- h. The Student Internet Use Policy shall be developed pursuant to this policy include requirements that address the following safe and responsible use issues:
 - i. Access to inappropriate material.
 - ii. Privacy and communication safety standards for self and others.
 - iii. Illegal activities, including computer security violations, actions taken to disrupt the performance of a computer system, and the use of the Internet to engage in other criminal acts.
 - iv. Inappropriate language.
 - v. Plagiarism and copyright infringement.
 - vi. Actions or use that may disrupt or jeopardize the security or effective performance of the District's network or the Internet.
 - i. The District will protect against the unauthorized disclosure, use, or dissemination of personal or confidential information of students.
 - j. The District will review contracts with third party providers of data management services to ensure compliance with federal and state student privacy laws.
 - k. The District will develop regulations for teachers/staff pertaining to the transmission of student confidential information via direct electronic communications to ensure that such transmissions are in compliance with the federal and state student privacy laws.
 - l. The District will develop regulations for teachers/staff and students to ensure the protection of student personal information when accounts are established or information is provided by or about students on third party web sites.
 - m. The District will develop regulations addressing the disclosure of student information, posting student-created material, and posting pictures of students on the District web site.
6. Each school will provide an annual written notice to the parents/guardians of students about the District Internet system, the policies governing its use, and the limitation of liability of the District. Parents/guardians must sign an agreement to allow their child to access the Internet. Parents/guardians have the right to request the termination of their child's Internet access at any time.
7. The District will implement an Internet records retention system.
8. The District will develop copyright management regulations that will protect the rights of copyright holders, including students and teachers/staff, related to material that is accessed through or placed on the Internet.
9. The District will develop District web site regulations to promote the effective educational use of the Internet, protect the privacy rights and other rights of students and teachers/staff, limit potential liability of the District for the inappropriate placement of material, and present an image that will reflect well on the District, schools, teachers/staff, and students.

10. The administrative responsibilities of the District administrative staff related to the District Internet system are as follows:
- a. The Superintendent, or his/her designee, will serve as the coordinator to oversee the District Internet system. The Superintendent is authorized to develop regulations and agreements for the use of the District Internet system that are in accord with this policy statement, and other District policies.
 - b. The site administrator, or his/her designee, will serve as the site-level coordinator for the District Internet system, will develop site-level regulations necessary to implement this policy and District regulations, establish procedures to ensure adequate supervision of students using the system, maintain executed user agreements, and be responsible for interpreting this policy and related regulations at the building level.
 - c. The District's Technology Advisory Committee will be responsible for ongoing evaluation of the issues related to this policy, related regulations, and the strategies implemented by schools under this policy. The District's Technology Advisory Committee will solicit input and feedback from teachers/staff, students, parents/guardians, and the community in this evaluation process.

Legal References:

Children's Internet Protection Act (CIPA), 47 U.S.C. 254
Copyright Law of the United States, Title 17 U.S.C
Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510, et. seq.
Family Education Rights and Privacy Act (FERPA), 20 U.S.C. 99, et. seq.
Federal Rules of Civil Procedure 26
California Education Code 7054
California Education Code 48901.5
California Education Code 49073 — 49079
California Education Code 51871.5
California Department of Education's Acceptable Use Policy Guidelines

Policy Adopted: August 27, 2008

I. DISTRICT'S INTERNET LIMITED PURPOSES

A. EDUCATIONAL PURPOSE

The District's Internet system has a limited educational purpose.

1. The term *educational purpose* includes use of the system for administrative and classroom activities, continuing education, professional or career development, and high-quality, educationally enriching personal research.
2. Students may not use the system for personal and/or personal commercial purposes, including offering or purchasing products or services.
3. 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 as individuals.

B. BUSINESS PURPOSE

The District's Internet system has a limited business purpose.

1. The term "business purpose" includes, but not limited to, use of the system for vendor management, purchasing, business correspondence, professional or career development, attendance, grading, investigations, Board activities, discipline and other business of the District.
2. Staff may not use the system for personal commercial purposes including, but not limited to, offering or purchasing products or services.
3. Staff may use the system for personal use if such use is limited.
4. Staff may use the District Internet system for communications related to acceptable collective bargaining and union organizational activities in compliance with fair labor practices.
5. A school may not establish an after school "open access" program or enter into an agreement with an authorized after school activities provider to all open access to the Internet unless authorized by the Superintendent or designee. If authorized, all such programs will be monitored by the school site administrator or designee.

II. RIGHTS AND RESPONSIBILITIES

A. GENERAL

It is the goal of the District to maintain an environment that promotes the ethical use and responsible conduct in all online network activities by staff and students. The District recognizes its legal and ethical obligation to protect the well-being of students in its charge. To this end, the District retains the following rights and recognizes the following obligations:

1. To deploy a Wide Area Network that will allow staff and students to communicate with each other and throughout the world. Additionally, this network will provide the

staff and students access to a multitude of administrative and instructional resources from both local and remote repositories of electronically stored information.

2. To log network use and to monitor fileserver space utilization by users.
3. To monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
4. To provide internal and external controls as appropriate and feasible. Such control shall include the right to determine who will have access to the District's-owned equipment and, specifically, to exclude those who do not abide by the District's acceptable use policy or other policies governing the use of school facilities, equipment and material. The District reserves the right to restrict online destinations through software or other means.
5. To provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing online communications.

B. STAFF RESPONSIBILITIES

1. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the District.
2. Staff should make reasonable efforts to become familiar with the Internet and its use so that effective use of these information and communication technology resources may be achieved.

C. USER RESPONSIBILITIES

Use of electronic media provided by the District is a privilege that offers a wealth of information and resources for research. Where it is available, this resource is offered to staff and students at no cost. In order to maintain the privilege, users agree to learn and comply with all provisions of the governing policies and regulations.

III. ACCEPTABLE AND UNACCEPTABLE USE

A. ACCEPTABLE USE

1. All use of the Internet must be in support of business, educational and research objectives consistent with the mission and objectives of the District.
2. Proper codes of conduct in electronic communication must be used. When using e-mail, blogs, wikis or online discussion groups, extreme caution must always be taken in revealing any information of a personal nature.
3. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.
4. All communications and information accessible via the network should be assumed to be private property.

5. Exhibit exemplary behavior on the network as a representative of one's school and the community. Be polite.
6. From time-to-time the District will make determinations on whether specific users of the network are consistent with the acceptable use practice.

B. UNACCEPTABLE USE

1. Giving out personal information about another person, including home address and telephone number, is strictly prohibited.
2. Gaining unauthorized access to computer systems or files is prohibited.
3. Password sharing and account trespassing are strictly forbidden and such acts will result in disciplinary action.
4. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
5. Any use of the network for commercial or for-profit purposes is prohibited.
6. Excessive use of the network for personal business shall be cause for disciplinary action.
7. Any use of the network for product advertisement or political lobbying is prohibited. Students and staff may communicate with elected representatives to express views on political issues.
8. No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.
9. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage software components of a computer or computing system is prohibited.
10. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.
11. The installation of any illegal or unlicensed software, including shareware and freeware, for use on District computers is prohibited. Installation of shareware without compensation to its originator will be considered a violation of this provision.
12. Use of the network to access or process pornographic material, inappropriate text files (as determined by the Superintendent or designee, or school site administrator), or files dangerous to the integrity of the local area network is prohibited. Any user who inadvertently accesses material that is considered prohibited or restricted should immediately disclose the inadvertent access to the Technology Department at techsvsdesk@fremont.k12.ca.us through a teacher or site administrator if necessary. This will protect the user against an allegation that he/she has intentionally violated this provision.
13. Downloading, copying, or otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited,

- except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law. (Title 17, United States Code)
14. Use of the network for any unlawful purpose is prohibited; this includes but is not limited to, such things as “hacking” or “cracking”.
 15. Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.
 16. Playing games is prohibited unless specifically authorized by a school site administrator or teacher for instructional purposes.
 17. Establishing network or Internet connections to live communications, including voice and/or video (relay chat), is prohibited unless specifically authorized by the Superintendent or designee.
 18. The use of external proxy servers or similar technologies to bypass or seek to bypass the District’s filtering software, a.k.a. Technology Protection Measure.

IV. UNLAWFUL, UNAUTHORIZED, AND INAPPROPRIATE ACTIVITIES

A. UNLAWFUL ACTIVITIES

Users are responsible for respecting all local, state and federal laws while using District computers, while operating on the District’s network and while on the Internet.

1. Users will be in violation of District policies, and applicable laws, if they attempt to gain unauthorized access to the District Internet system/network or to any other computer system through the District system, or go beyond their authorized access. This includes, but is not limited to, attempting to log in through another person's account or access another person's files.
2. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.
3. Users will not use the District Internet/network system to engage in any other unlawful act including, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal and gang activity, and threatening the safety of person.

B. INAPPROPRIATE LANGUAGE

1. Restrictions against inappropriate language apply to all speech communicated through the District Internet system, including but not limited to public messages, private messages, material posted on web pages or blogs, or posted in any other manner.
2. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
3. Users will not post information that, if acted upon, could cause damage or a danger of disruption to the District, a school, or any other organization or person.

4. Users will not engage in personal attacks including, but not limited to, prejudicial or discriminatory attacks.
5. Users will not harass or bully another person.
6. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
7. Students will promptly disclose to their teacher or another school employee any message they receive from any other student that is in violation of the restrictions on inappropriate language. Students should not delete such message until instructed to do so by the school site administrator or designee. The Technology Department may be called upon to conduct a technical investigation, if necessary.

C. PLAGIARISM AND COPYRIGHT INFRINGEMENT AND TRAINING

1. Users will not plagiarize works that they find on the Internet.
2. Users will respect the rights of copyright owners in their use of materials found on, disseminated through, or posted to the Internet.
3. School site administrators will establish professional development and/or training for staff relative to the education of teachers and students on copyright and plagiarism in accordance with California Education Code 51871.5.
 - Staff and students will be educated on the appropriate and ethical use of technology in the classroom, Internet safety, avoiding plagiarism, the concept, purpose and significance of a copyright so that pupils can distinguish between lawful and unlawful online downloading, and the implication of illegal peer-to-peer network file sharing.

V. SYSTEM SECURITY AND RESOURCE LIMITS

A. SYSTEM SECURITY

1. 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.
2. Users will immediately notify the Technology Department, if they have identified a possible security problem. However, users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
3. Users will avoid the inadvertent spread of computer viruses by following the District virus protection procedures as outlined in the Student and Employee Use Agreements.
4. Users may not engage in activities designed to circumvent user authentication or security of any host, network, or account (referred to as “hacking” or “cracking”), reverse engineer, decompile, deconstruct any programming, nor interfere with service to any user, host or network. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.

5. Users shall not abuse, destroy, or modify hardware and/or software in any way.
6. Only District computing equipment approved by the Technology Department may be connected to the District's network.
 - a. Personal employee laptops and vendor computers may be used if approved in writing. Users may apply for said exception by submitting a Use of Personal Computer on District Network form to the Technology Department. A link to the form can be found on the Technology Department's web page. The completed form should be submitted to the Technology Department. The request must be approved prior to connection to the District's network.
 - b. Consumer-grade wireless access points may not be connected to the District's network unless authorized by the Technology Department. Requests for such installation must be submitted using the Technology Work Request system, found at www.myschoolbuilding.com. Authorized wireless access points must be secured, i.e., password protected, and must adhere to the District's IP numbering convention.

B. RESOURCE LIMITS

1. Due to bandwidth constraints, 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, such as at the end of the school day, and immediately remove the file from the system computer to their designated/assigned electronic file, diskette, compact disk, or other storage medium.
2. Users will not misuse District, school, or personal distribution lists or discussion groups for sending irrelevant messages.
3. Users will check their e-mail frequently, delete unwanted messages promptly, and stay within their allocated e-mail storage space capacity.
4. Users will subscribe only to approved, high quality discussion groups that are relevant to their education or professional/career development.
5. Excessive use of the District Internet system may raise a reasonable suspicion that the employee or student is using the system in violation of District governing policies and regulations.
6. Computers which a student will use an appropriate pop-up blocker to block advertising that may be connected to a web site. Computer lab personnel will ensure all computers within the lab have the pop-up blocker on at all times. Teachers and computer lab personnel may temporarily disable said pop-up blocker if the blocking software hinders instruction.

VI. PROMOTING THE EFFECTIVE EDUCATIONAL USE OF THE INTERNET

- A. The District will provide professional development opportunities for teachers and administrators to help them learn how to use computers and in the effective use of the Internet for instructional purposes, disseminate Internet-based lesson plans, and provide technical and instructional support to students

1. Substitute teacher must be specifically certified to instruct in classroom where students are accessing the Internet. Certification requirements will ensure that substitute teachers have a standard level of technical proficiency and understand Internet safety and responsible use issues, this policy and regulation and the obligations related to supervision of students in their use of the Internet.
 2. Unless they are under the direct supervision of their cooperating teacher, student teachers must be certified to instruct classrooms where students are accessing the Internet.
- B.** All sites linked 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.
- C.** The District, school site administrators, 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, school or teacher web sites or other assignments utilizing the Internet.
- D.** 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/staff. Prescreening will be accomplished by the school site administrator or designee who will prepare and maintain a roster of prescreened sites, date when screened and the name of the screener.
- E.** Schools shall develop written rules and procedures for student access to web sites and shall promulgate these rules and procedures to the students through the teachers' professional development and/or training. Said rules and regulations shall be reviewed annually by the school site administrator for current applicability.

VII. PROTECTIONS AGAINST ACCESS TO INAPPROPRIATE MATERIAL

A. INAPPROPRIATE MATERIAL

1. The District has identified the following types of material as Prohibited, Restricted, and Non-educational Material.

- a. Prohibited Material

Prohibited Material may not be accessed by the students, teachers, 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.

- b. 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 Superintendent or designee.

c. Non-Educational Material.

Non-educational Material is material that is generally considered to be of no educational value or entertainment. Non-educational Material may be accessed in the context of specific learning activities that are directed by teacher/staff. Non-educational Material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investments.

2. Any user who inadvertently accesses material that is considered Prohibited or Restricted should immediately disclose the inadvertent access through a teacher or site administrator. This will protect the user against an allegation that he/she has intentionally violated the policy.
3. The determination of whether material is Prohibited, Restricted, or Non-educational will be based on the content of the material and the intended use of the material, not on the protective actions of the Technology Protection Measures. The fact that the Technology Protection Measures have 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 Measures have protected access to certain material shall not create the presumption that the material is inappropriate for users to access.

B. TECHNOLOGY PROTECTION MEASURES

1. General

- a. Technology Protection Measures 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 in consultation with schools may, from time-to-time, reconfigure the Technology Protection Measures to best meet the educational needs of the District or schools and address the safety needs of the students.
- b. Technology Protection Measures 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 Department may disable said measure for system administrative and maintenance purposes when students are not using the system.

- c. Students' free speech rights of access to information within an educational environment shall be fully protected. Care will be taken in the selection and configuration of the Technology Protection Measures to ensure that viewpoint discrimination does not occur.
 - d. Students and staff may not use external proxy servers or similar technologies to bypass or seek to bypass the filtering software.
 - e. The Chief Technology Officer will conduct an annual analysis of the effectiveness of the selected technological protection measures and make recommendations to the Superintendent regarding selection and configuration.
 - f. The Chief Technology Officer will provide a monthly written report to the Superintendent outlining all requests for modification of the technological protection measures and any resulting changes.
2. Unblocking Web Sites
- a. Technology Protection Measures have been found to inappropriately block access to appropriate material from time-to-time. To ensure that the implementation of the Technology Protection Measures 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/staff or students, and ensures the protection of students' constitutional rights of access to information and ideas, authority will be granted to school site administrators or designees to temporarily unblock access to sites blocked by the Technology Protection Measures when technically feasible.
 - b. Authority to temporarily unblock access will be granted to the site administrators or designees. Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are necessary to ensure the security of the system. The Superintendent or designee shall determine such standards. If the authorized site administrator is unavailable, staff may call the Technology Service Desk at internal line 12-611 and request the temporary unblocking of a web site.
 - The authorized school site administrator must review the contents of the site, outside of the presence of any student, prior to allowing access to the site by a student.
 - The authorized school site administrator will report all instances of temporary unblocking to the Technology Department's Service Desk within one (1) school day as the unblocking occurred. Such actions will be included in the Chief Technology Officer's monthly report to the Superintendent.
 - c. If an authorized individual believes that the blocked site should be permanently unblocked, a written request will be forwarded to the Chief Technology Officer.
 - The written request for unblocking a web site will include:
 - Requester's name, school/district site, and title
 - Requester's phone number

- Complete web address of website requesting to be unblocked
 - Educational purpose and educational value of the web site
 - After investigation by technology personnel, the Chief Technology Officer may make a decision to permanently unblock access to the site or may delegate the decision to the District's Instructional Services Division. Decisions about unblocking should generally take no longer than one school day.
- d. A list of all web sites that have been permanently unblocked, together with the rationale for making the decision to unblock the site, will be forwarded monthly, as necessary, to the Superintendent, the District Instructional Services Division, school site administrators, and the Technology Service Desk.
3. Blocking Web Sites
- a. Technology Protection Measures have been found to inappropriately unblock access to inappropriate material from time-to-time. Current Technology Protection Measures do not permit delegation of web site blocking to the school site level; therefore, any requests to have a web site blocked will go through the Technology Department.
- b. Any staff member, parent/guardian or student may request the Technology Department block a web site. Notification may be made to the Service Desk via telephone at 12-611 or e-mail techsvs@fremont.k12.ca.us; or to the Chief Technology Officer's office at (510) 659-2575.
- The request for blocking a web site will include:
 - Requester's name, school/district site and title
 - Requester's phone number
 - Complete web address of website requesting to be blocked
 - Reason why the requester believes the web site should be blocked
- c. Upon receipt of a request to block a web site, the Service Desk representative or other designated Technology Department staff member will immediately suspend access to the web site pending a Technology Department review.
- d. Once a review is completed and documented it will be presented to the Chief Technology Officer. The Chief Technology Officer may authorize the permanent blocking of the web site. The web site may be referred to the Instructional Services Division if the Chief Technology Officer is not available, if requested by the requestor or if the Chief Technology Officer disagrees that the web site should be blocked.
- e. A list of all web sites that have been permanently blocked, together with the rationale for making the decision to block the site, will be forwarded monthly, as necessary, to the Superintendent, the District Instructional Services Division, school site administrators, and the Technology Service Desk.

4. Overriding the Technology Protection Measures

- a. In order to provide access to educational resources located on the Internet, the Technology Department may provide a means to override the technology protection measures (i.e., filters). The override will allow for the temporary disabling of the filter for a specific individual for a specific period of time.
- b. The following conditions apply.
 1. The following staff may obtain override codes.
 - a. Teachers
 - b. Principals and Administrators
 - c. School Resource Officers
 - d. Counselors
 - e. Nurses
 - f. District Office Directors
 2. Overrides must be requested in writing, by the staff member and approved by the principal.
 3. Overrides shall be limited time to no more than one (1) hour per session.
 4. Override codes shall be good for no more than one (1) school year.
 5. Staff receiving codes shall be required to sign an *Acknowledgement of Responsibilities* form once a year for every year an override is requested.
 6. Overrides shall not be used on more than one computer at a time.
 7. Override user shall remain at the computer at all times during the override session.
 8. Override user shall log out of the override session immediately upon end of use.
 9. Override user shall ensure compliance with the terms and conditions set forth throughout this administrative regulation and all Board policies and administrative regulations pertaining to technology use and safe operation.
 10. Students shall not be permitted to have access to override codes.
 11. Students shall not have access to a computer on which an override is currently running.
 12. Overrides shall be used strictly for educational purposes, bona fide research, or other lawful purposes, as stipulated in the Children's Internet Protection Act. Override codes shall not be used for personal purposes.
 13. Users shall report any suspected compromises or security breaches of the override code to the Technology Department immediately upon discovery.
- c. Users shall attempt to avoid audio and video streaming during the school day due to bandwidth limitations. Staff is encouraged to download audio/video clips to a local hard drive prior to class in order to ensure the best quality sound and image. Exceptions to this shall be during breaking stories deemed relevant to the class

subject matter. Staff is encouraged to use the Educational Video Library to download and store videos for recurring use so as to keep bandwidth use to an acceptable level. In using the Educational Video Library videos may be shared between teachers and may serve as a valuable teaching resource.

- d. Override code recipients and users shall understand and acknowledge that:
 1. There is no expectation of privacy while using any government computing equipment including but not limited to, computers, servers, wide area network, local area networks, and printers;
 2. Override use shall be monitored by the Technology Department; and
 3. Periodic override activity reports on override code use, including but not limited to, site(s) visited, name of person visiting the site, and date and time of visit shall be developed and sent to the Superintendent by the Technology Department, as appropriate. Reports may also show any concurrent use of the override.
- e. Improper use of the override code is subject to discipline up to and including termination.

VIII. SUPERVISION, MONITORING, SEARCH AND SEIZURE, AND RETENTION OF RECORDS

A. SUPERVISION

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 school site 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.

B. MONITORING

1. The District will monitor student and staff use of the Internet through a regular analysis of Internet usage. Depending upon the availability of funds, school site administrators may implement additional computer monitoring software, as desired. This software will be standardized throughout the District and coordination of the purchase and installation will be made through the Technology Department.
2. Users should have no privacy expectations in the contents of their files and records of their online activity while on the District system, or using or saving said data on District equipment.

C. SEARCH AND SEIZURE

1. 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 if there is reasonable suspicion that such violations have occurred.

2. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation. Individual search of user's e-mail will first be approved by the District administrator responsible for supervision of the student or staff member or by the Superintendent or designee.
3. In the event an individualized search is conducted, a record will be established detailing the reason for the search, the extent of the search, and the results.

D. RETENTION OF RECORDS

1. The Superintendent, or designee, will implement an Internet records retention system to include but not limited to, e-mail messaging, which is in accordance with state and federal law. The District will comply with the Federal Rules of Civil Procedure (FRCP) 26 relative to the retention of government e-mail and electronic documentation. E-mail and other message files will be retained for a period of three (3) years, space permitting, and then purged from the system.
2. Any other Internet records that are not subject to regulatory retention requirements will be destroyed after one (1) year.
3. Site administrators will regularly inform staff that the contents of their files may be discoverable under state public records laws and the Federal Rules of Civil Procedure.

IX. ELECTRONIC COMMUNICATION

A. STUDENTS

1. Students who have provided the District a Student Use Agreement signed by the student and parent/guardian will be permitted to access the Internet through the District system.
 - a. Parent/Guardian may revoke this authorization anytime by contacting the Technology Department or school site administrator.
 - i. If received by the Technology Department, the Service Desk will inform the school site administrator. Technology Department will take immediate steps to terminate access and will inform the school site administrator.
 - ii. If received by the school site administrator, the Technology Department will be immediately notified of the revocation.
 - iii. The school site administrator will take immediate steps to ensure the revocation is enforced by notifying the student's teachers, library media technicians, computer lab employees, and all other appropriate personnel of the revocation.
2. The District will not provide District e-mail accounts for students using the District's e-mail system.
 - Students may establish or access web-based e-mail accounts on commercial services through the District Internet system only when such accounts have been

approved for use by the school site administrator or designee and the Superintendent or designee.

3. Students may use real-time electronic communication, such as chat, only under the direct supervision of a teacher or in moderated environments, supervised by staff, which has been established to support educational activities and have been approved by the Superintendent or designee.

B. STAFF

1. Staff will be provided with individual e-mail accounts. Staff will use a signature file that identifies who they are and their position with the District. Staff use of these District e-mail accounts will be for professional purposes.
2. Staff who have provided the District a signed Employee Use of Technology Agreement will be permitted to access the Internet through the District system.

X. PROTECTION OF STUDENT CONFIDENTIALITY AND PRIVACY

A. CONTRACTS

1. All contracts with third party providers of pupil products and services and data management services for the District will be reviewed to ensure compliance with federal and state student privacy and records retention laws.
2. Contracts that involve the transmission of student directory information or pupil confidential pupil record information must use the District's Master Agreement for Student Products and Services. Vendor management is the responsibility of the Director of Pupil Services. No contract may be entered into without the contract going through the Director of Pupil Services.
3. The safe and secure transmission of student confidential information to vendors is the responsibility of the Technology Department. Transmission of said information to vendors will only be accomplished if a Master Agreement has been properly executed through the Pupil Services Department. A copy each executed Master Agreement will be on file in the Technology Department.

B. ELECTRONIC MAIL (E-MAIL)

1. Staff transmission of student confidential information via e-mail must be in compliance with all federal and state student privacy laws.
2. Staff members whose job requires the transmission of student confidential information via e-mail shall be trained by the Technology Department in the proper procedure are authorized to transmit said data.
 - a. The "subject line" of the e-mail should provide an indication that the e-mail contains confidential student information.
 - b. Confidential information will only be sent as an attachment to the e-mail. The attachment must be properly secured for transmission.

- c. A hard copy of any e-mail containing student confidential information will be retained in accordance with District student records retention requirements.

C. STUDENT ON-LINE ACCOUNTS

Teachers will ensure the protection of student personal information when establishing any relationship with a third-party site or system.

1. Teachers/Staff may require, encourage, or allow students to establish individual accounts on a third party site or system only under the following circumstances:
 - a. The establishment of the account is necessary to achieve an identified educational purpose.
 - b. Student personal information and student use data will not be collected, analyzed, and/or used for commercial advertising or marketing purposes.
 - c. A minimum amount of non-identifying information is collected for the purpose of establishing the account.
 - d. The third party system has committed to maintain the privacy of any information provided.
 - e. The third party system provides a process by which the District or a parent/guardian may access, review, and remove their student's account information.
2. Signed parental/guardian permission must be obtained prior to the establishment of the student account. Notice to the parent/guardian about proposed student accounts on third party systems must include the following information:
 - The name, full URL (web address), and privacy policy of the third party system.
 - Description of the educational purpose for the establishment of the account.
 - The period of time for which the account will be established.
 - Information on how they can access their student's records on the third party site.

D. PRIVACY AND COMMUNICATION SAFETY STANDARDS

1. 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. Elementary and junior high school students will not disclose their full names or any other personal information for any purpose.
 - b. High school students will not disclose personal contact information except to educational institutions for educational purposes, companies, or other entities for career development purposes, or with specific staff approval or except with Superintendent approval.
 - c. Students will not disclose names, personal contact information, or any other private or personal information about other students under any circumstances.

- 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 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 teacher or staff member, and then only with permission of the school site administrator. The Technology Department may be contacted to conduct an investigation, as appropriate.
2. The following provisions address the disclosure of student information, posting student-created material, and posting pictures of students on the District web site or any school web site. The District or schools may establish password-protected web sites that will restrict access to staff, students, and their parents/guardians. Parent/guardians must approve any disclosure of student identifying information and posting of student-created material.
- a. For elementary and junior high students, the following standards apply to any material posted on a publicly accessible site:
 - Students will use a username that will disguise their full name.
 - 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 student's surname.
 - b. For elementary and junior high students material posted on a password-protected site, parents/guardians may approve the elementary and junior high school standards for publicly accessible sites or the following standards:
 - Students may be identified by their full name.
 - Group and individual pictures of students with student identification are permitted.
 - Student work may be posted with student name.
 - All student-posted work will contain the student's copyright notice including the student's name.
 - c. For high school students material posted on publicly accessible sites or password-protected sites, parents/guardians may approve either the elementary and junior high school standards or the following standards:
 - Students may be identified by their full name.
 - Group and individual pictures of students with student identification are permitted.
 - Student work may be posted with student name.
 - All student-posted work will contain the student's copyright notice including the student's name.

XI. COPYRIGHT MANAGEMENT

A. EMPLOYEES AND STUDENTS

1. The District will respect the copyright rights of students and employees.
2. Students own the copyright to their creative works, including works created using District resources. The Internet agreement signed by parent/guardians will include a request for permission from parents/guardians 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.
3. District employees own the copyright to works created outside of the scope of their employment responsibilities and without the use of District resources. District employees may post such work on the District web site to facilitate access by students and/or employees. Notice of such posting and claim of ownership must be provided to the Superintendent or designee. By posting such work to the District's web site, the employee will grant a non-exclusive license and/or permission for any employee or student within the District to freely use such work.
4. The District shall own the copyright on any works created by District employees within the scope of their employment responsibilities and shall be considered as work for hire unless specified by collective bargaining agreement.

B. COPYRIGHTS OF OTHERS

1. The District will promote respect for the copyright rights of others.
2. The District will provide instruction to employees and students on their rights and responsibilities with respect to the copyright ownership rights of others.
3. 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 accordance with the fair use provisions of the copyright law, or is disseminated or posted with written permission of the copyright owner. Said permission will be kept on file by the web sites designated webmaster.

XII. WEB SITE REGULATIONS

A. DISTRICT WEB SITE

1. The District will establish a District web site. Material appropriate for placement of the District web site includes: District information, school information, teacher and class information, student projects, and student extracurricular organization information. Personal information unrelated to education will not be allowed on the District web site.
2. The Superintendent will designate a District webmaster to be responsible for maintaining the official District web site and monitoring all District web activity. The webmaster will develop style and content guidelines for official District and school web materials and develop procedures for the placement and removal of such material.

3. All official District material originating from the District posted on the District web site must be approved through a process established by the District webmaster.

B. SCHOOL WEB PAGES

1. The school site administrator will designate a school webmaster, responsible for managing the school web site and monitoring class, teacher, student, and extracurricular web pages.
 - a. All official material originating from the school will be consistent with the District style and content guidelines as established by the District webmaster and approved through a process established by the school webmaster.
 - b. The school webmaster will develop additional guidelines and placement processes for the school web site approved by the school site administrator. All other web pages shall be a closed forum.
 - c. There shall be complete school control of all posted web information.
2. It will not be considered a violation of a 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 governing policies, administrative regulations or collective bargaining agreements.
3. The District reserves the right to remove any web site from the District network at any time.

C. TEACHER AND CLASSROOM WEB PAGES

1. Due to equipment capacity limitations, teacher and classroom web pages cannot be currently hosted on the District network. The Technology Department will strive to provide such capability in the future within the equipment capacity limitations and fiscal constraints of the department.
2. When technically feasible, teachers may establish web pages, blogs, wikis and forums for use with class activities or that provide a resource for other teachers. The Superintendent, or designee, will establish standards for teacher and classroom web pages including, but not limited to, the maximum size, format and appropriate content. School site administrators may establish further standards which do not exceed the established District standards.
3. Teachers' web sites will adhere to the general look and feel, and content restrictions of the District and school web site guidelines. Teachers will be responsible for creating and maintaining their class or educational resource sites.
4. Teacher web pages will be developed in such a manner as to reflect well upon the District and school.
5. It will not be considered a violation of a teacher'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 governing policies, administrative regulations or collective bargaining agreement.

6. The District reserves the right to remove any teacher web site from the District network at any time.
7. Teacher web sites may remain active beyond the school year. School site administrators, or designee, will review each teacher's web site for adherence to the governing policies, administrative regulations and standards on a periodic basis but not less than annually.
8. Teacher web sites hosted outside of the District's network will comply with this administrative regulation as long as it represents the views of the District.

D. STUDENT WEB PAGES

1. Due to equipment capacity limitations, student web pages cannot be currently hosted on the District network. The Technology Department will strive to provide such capability in the future within the equipment capacity limitations and fiscal constraints of the department.
2. When technically feasible, students may create web sites and blogs as part of a specific instructional activity. Material presented on student web pages and blogs must meet the educational objectives of the instructional activity. Such pages shall be strictly limited to the educational objectives and subject to the individual limitations of the school for that activity.
3. Student web pages and blogs will be created, maintained under the direct supervision of a teacher or supervising staff member.
4. Student web pages will be monitored by the teacher/staff member permitting the activity, the school site webmaster and the school site administrator.
5. 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 governing policies, administrative regulations, or student discipline policies and regulations.
6. The District reserves the right to remove any student web site from the District network at any time.
7. 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.
8. Student web sites must be taken down at the end of the school year or earlier if the instructional activity has ended. The Technology Department may remove any remaining student web pages at the end of the school year without further notice.

E. EXTRACURRICULAR ORGANIZATION WEB PAGES

1. With the approval of the school site administrator, extracurricular organizations, such as athletic booster clubs, may establish web pages. Material presented on the organization web page must relate specifically to organizational activities.
2. Organizational web pages must include the following notice.

This is an extracurricular organization web page. Opinions expressed on this page shall not be attributed to the District.

3. It will not be considered a violation of a 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 governing policies, administrative regulations or bargaining unit agreement.
4. The District reserves the right to remove any extracurricular organization's web site from the District network at any time.

F. WEB PAGE REQUIREMENTS

1. All web pages associated with the District are considered to be a limited public forum. All material posted on the web pages using the District domain will be developed in such a manner as to reflect well upon the District and its schools, staff and students.
2. All new District web sites, blogs, wikis and forums, and all school, class and distance education materials will be fully compliant with disability information technology access standards. The District will develop a plan to revise all existing web site material to achieve compliance with access standards.
3. All Internet governing policies and administrative regulations 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.
4. Web pages, blogs, wikis and forums 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.
5. Material placed on the web site is expected to meet academic standards of proper spelling, grammar, and accuracy of information.
6. 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.
7. 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.

G. WEB SITE CONCERNS

The District web site and each school, teacher, student and extracurricular organization web page will have a "Web Site Concerns" link. This link will take the reader to a page that provides the following information:

Fremont Unified School District seeks to ensure that all materials placed on the District or school web sites are placed in accordance 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. <hyperlink to policy goes here>*
- *We have established web site management procedures to review materials prior to their placement on the web site. <hyperlink to procedures goes here>*
- *We will promptly respond to any issues of concern. If you have a concern about material placed on our web site, please contact us. <hyperlink to e-mail of an administrator who has the responsibility of promptly responding to any complaint goes here>*

XIII. ELECTRONIC SIGNALING DEVICES

1. Electronic signaling devices, including but not limited to cellular telephones, pagers and personal digital assistants (PDA), are to be silenced and stored during school hours unless teacher or school site administrator permission has been secured.
2. Any student who violates the electronic signaling device policies, regulations and procedures of the District, may have his/her electronic signaling device confiscated by school personnel. Students who possess electronic signaling devices on school property understand that the District shall not be liable for any lost or stolen devices including those which are confiscated. If the privilege of using these devices at school is abused and the possession or use of electronic signaling devices violates this regulation, the school shall revoke the privilege and prohibit a student from possessing such devices.
3. No student shall be prohibited from possessing or using an electronic signaling device that is determined, and documented, by a licensed physician and/or surgeon to be essential for the health of the student and use of which is limited to purposes related to the health of the student (Ed. Code 48901.5). A student must provide documentation of medical need to the school administration in advance of any such use of electronic signaling devices. A copy of said documentation will be forwarded to the Director of Pupil Services.
4. Any electronic signaling device requiring Internet connectivity as a means of communications to the physician's office must provide a request for Internet connectivity, signed by a licensed physician and/or surgeon, to the Chief Technology Officer and Director of Pupil Services.

XIV. DUE PROCESS

1. The District will cooperate fully with local, state and federal officials in any investigation involving or relating to any unlawful activities conducted through the District's Internet system and District equipment.
2. In the event of an allegation that a student has violated governing policies or administrative regulations, the student will be provided with notice and an opportunity to be heard in the manner set forth in the student disciplinary code.

3. In the event of an allegation that an employee has violated governing policies or administrative regulations, the matter will be handled in accordance with District policies and collective bargaining agreements.

XV. FACILITIES LEASE/RENTERS USERS AND CHARTER SCHOOLS

A. FACILITY LEASERS/RENTERS

1. Lease and Facility Rental Agreements of District facilities will not generally authorize access to the District's network or computer equipment.
2. In the event that the terms of the lease or rental agreement include access to the District's Internet system, the conditions of the governing policies and this regulation shall apply.
 - a. Access will be restricted to Internet access only and not to the District Internet System for Internet connectivity and will not include District computing equipment.
 - b. Additional fees for said access and related technical service support may be imposed.
3. Installing any wireless device in order to gain access to the District Internet System or District Network is prohibited
 - a. Wireless Internet access through a third party commercial provider which does not access the District's Internet system may be used.

B. CHARTER SCHOOLS

1. Providing access to District facilities to charter schools does not automatically include access to the District's Internet system or computing equipment. In the event that a charter school obtains permission to utilize District computing equipment and/or Internet system, the provisions of the governing policies and administrative regulations shall apply.
2. Fees for said access and related technical service support may apply.
3. Installing any wireless device in order to gain access to the District Internet System or District Network is prohibited
 - a. Wireless Internet access through a third party commercial provider which does not access the District's Internet system may be used.

XVI. DEFINITION OF TERMS

- District Equipment. Any and all District-owned equipment including, but not limited to, computers and peripherals, printers, scanners, servers, switches, hubs, optical fiber and copper wiring and wireless systems.
- District Internet System. Any and all portions of the District's Wide Area Network or Local Area Networks equipment and peripherals.

- District Network. Any and all portions of the District's technology backbone system including, without limitation, the District Internet system, business applications, software, databases and storage devices.
- Internet. A collection of interconnected computer networks around the world.
- Personal contact information. This includes a student's name together with other information that would allow an individual to locate a student, including, but not limited to, parent/guardian's name, home address or location, work address or location, or phone number.
- Technological Protection Measures. These measures include technologies that seek to block user access to certain sites (filtering software), block inappropriate material from being sent to direct users, ensure the security of the District network and monitors Internet use.
- Staff. Any employee including, but not limited to, certificated employees, classified employees, para-educators, coaches, teaching assistants, nurses, counselors, volunteers, administrators, classified managers, and contract employees.
- Student. Any individual attending any Fremont Unified School District school.

XVII. DISCLAIMER

1. The District cannot be held accountable for the information that is retrieved from the Internet.
2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all electronic mail and traffic, and have the ability to monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
3. The District will not be responsible for any damages suffered by any user, including loss of data resulting in delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.
4. The District makes no warranties, expressed or implied, with respect to:
 - a. The content of any advice or information received by the user, or any costs or charges incurred as a result of seeing or accepting any information; and
 - b. Any costs, liability, or damages caused by the way the user chooses to use his/her access to the network.
5. The District reserves the right to change its policies, regulations, standards, guidelines and rules at any time.

Business and Non-Instructional Operations
Internet Safe and Responsible Use

AR 3521.1
24 of 24

Regulation Established: August 27, 2008

Regulation Revised: February 10, 2010