

Title: Internet-Appropriate Student Use - Regulation

I. APPROPRIATE USE

1. The District's Internet system has a educational purpose.
 - a. The term educational purpose includes use of the system for classroom activities, continuing education, publishing, collaboration, and personal research.
 - b. Students may not use the system for personal commercial purposes, including offering or purchasing products or services.
 - c. The District may establish an after-school "open access" program or enter into an agreement with an authorized after-school activities provider to allow open access to the Internet for noneducational purposes. All student use during open access hours must be closely supervised. Students will be instructed that the District Internet use agreement will cover all use of the Internet during the "open access" program.

2. 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 and responsible independent use by older students.

3. The District will establish or authorize the use of a controlled communications environment that will allow the students to communicate electronically for educational purposes.

II. PROTECTIONS AGAINST ACCESS TO INAPPROPRIATE MATERIAL

1. Inappropriate Material
 - a. Students shall not intentionally access or download any text, file, or picture material, information or software, or engage in any conference other online activity that includes material which is illegal, defamatory, obscene, pornographic, libelous, indecent, vulgar, profane, or lewd or is otherwise harmful to minors; advertises any product or service not permitted to minors by law; constitutes insulting or fighting words, the

Title: Internet-Appropriate Student Use - Regulation

very expression of which injures or harasses others; or presents a clear and present likelihood that, either because of its content or the manner of distribution, it will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities or will cause the commission of unlawful acts or the violation of lawful school regulation

b. Any user who inadvertently accesses material that is considered prohibited or restricted should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the policy.

c. The determination of whether material is prohibited, restricted, or noneducational shall be based on the content of the material and the intended use of the material, not on the response of a technological protection measure. The fact that the technological 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 technological protection measure has blocked access to certain material shall not create the presumption that the material is inappropriate for users to access.

2. Technological protection measures

a. Technological protection measures include technologies that seek to block user access to certain sites (filtering software), block inappropriate material from being sent to District users, ensure the security of the District network, and monitor Internet use.

b. The District has selected technological protection measures for use with the District Internet system and has specified the manner in which these measures will be configured.

c. District filtering software 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 Privacy

Title: Internet-Appropriate Student Use - Regulation

Protection Act. The District or individual schools may, from time to time, reconfigure the technological protection measures to best meet the educational needs of the District or schools and address the safety needs of the students.

d. The District safety and responsible use committee will conduct a regular analysis of the effectiveness of the selected technological protection measures and make recommendations to the superintendent regarding selection and configuration.

3. Override, nondiscrimination, disabling, and bypass of filtering software

a. 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 protective actions of the filtering software.

b. The filtering software 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 filtering software may be disabled for system administrative purposes when students are not using the system.

c. Students may not use external proxy servers or other similar technologies to bypass or seek to bypass the filtering software.

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

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 a designee in each school will develop and disseminate staff supervision requirements. Computers used by students in classrooms and labs will be positioned to facilitate effective staff supervision.

2. The District will monitor student and staff use of the Internet through a regular analysis of Internet usage.

Title: Internet-Appropriate Student Use - Regulation

3. Users have no privacy expectation in the contents of their personal files and records of their online activity while on the District system. The District may supervise and monitor use of the District system and the activities of Users at any time, with or without notice.

4. Routine maintenance and monitoring of the system may lead to discovery that a user has violated or is violating District policy, regulations, or the law. An individual search will be conducted if there is reasonable suspicion that such violations have occurred. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

IV. ELECTRONIC COMMUNICATION

1. District employees will supervise and regularly review electronic communications of students.

V. UNLAWFUL, UNAUTHORIZED, AND INAPPROPRIATE ACTIVITIES

1. Unlawful activities

a. Users will not attempt to gain unauthorized access to the District 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 Internet system to engage in any other unlawful act.

2. Inappropriate language

a. Restrictions against inappropriate language apply to all speech communicated through the District Internet system, including public messages, private messages, and material on Web pages or in blogs, or posted in any other manner.

Title: Internet-Appropriate Student Use - Regulation

- 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 to the district, a school, or any other organization or person.
- d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- e. Users will not harass or bully another person.
- f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.
- g. 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 messages until instructed to do so by a staff member.

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.

VI. SYSTEM SECURITY AND RESOURCE LIMITS

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. However, users will not go looking for security problems, because this may be construed as an unlawful attempt to gain access.
- c. Users will avoid the inadvertent spread of computer viruses by following the district virus protection procedures.

Title: Internet-Appropriate Student Use - Regulation

VII. COPYRIGHT MANAGEMENT

1. The District will respect the copyright rights of students.
 - a. Students own the copyright to their creative works, including works created using District resources.
2. The District will promote respect for the copyright rights of other
 - a. The District will provide instruction to 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.

Approved: May 21, 1996

Reviewed: May 22, 2012

Revised: March 24, 2003
March 25, 2008
April 27, 2010
May 23, 2017