1. Instruction

1. Access to Electronic Networks [1]

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. [2] The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s). [3]

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. [4] Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyber-bullying awareness and response. [5] Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use. [6]

Acceptable Use [7]

---

[1] State or federal law requires this subject matter be covered by policy. State or federal law controls this policy's content. This policy contains an item on which collective bargaining may be required. Any policy that impacts upon wages, hours, and terms and conditions of employment, is subject to collective bargaining upon request by the employee representative, even if the policy involves an inherent managerial right. This policy concerns an area in which the law is unsettled.

[1] A policy on Internet safety is necessary to receive *E-rate* funds under the Elementary and Secondary Education Act, Enhancing Education Through Technology (20 U.S.C. §6751 et seq.) and to qualify for universal service benefits under the Children's Internet Protection Act (47 U.S.C. §254(h) and (l).

[2] This goal is repeated in exhibit 6:235-E2, *Authorization for Electronic Network Access*.

[3] Topics for the implementation plan include integration of the Internet in the curriculum, staff training, and safety issues. The implementation plan can also include technical information regarding service providers, establishing Internet accounts, distributing passwords, software filters, menu creation, managing resources and storage capacity, and the number of dial-up lines or access points for users to connect to their accounts. Another topic is investigation of inappropriate use.

[4] No system can guarantee to operate perfectly or to prevent access to inappropriate material; this policy statement attempts to absolve the district of any liability.

[5] Required by 47 U.S.C. §254(h)(5)(B)(iii) and 47 C.F.R. §54.520(c)(i) only for districts that receive *E-rate* discounts for Internet access or plan to become participants in the *E-rate* discount program. Beginning July 1, 2012, all boards receiving an *E-rate* funding for Internet access must certify that they have updated their Internet safety policies. See, *FCC Report and Order 11-125* (August 11, 2011). This sentence is optional if the district only receives discounts for telecommunications, such as telephone service, unless the district plans to participate in the *E-rate* discount program.

[6] School authorities may reasonably regulate student expression in school-sponsored publications for education-related reasons. Hazelwood School District v. Kuhlmeier, 108 S.Ct. 562 (1988). This policy allows such control by clearly stating that school-sponsored network information resources are not a "public forum" open for general student use but are, instead, part of the curriculum.

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein, or (2) for a legitimate school business purpose. Use is a privilege, not a right. [8] Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. [9] Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials. [10]

Internet Safety [11]

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. [12] The Superintendent or

---

[7] This paragraph provides general guidelines for acceptable use regardless of whether Internet use is supervised. The specific rules are provided in exhibit 6:235-E2, *Authorization for Electronic Network Access* (see also footnote 11). This paragraph's application to faculty may have collective bargaining implications.

[8] The "privilege, not a right" dichotomy is borrowed from cases holding that a student's removal from a team does not require due process because such participation is a privilege rather than a right. The deprivation of a privilege typically does not trigger the Constitution's due process provision. Clements v. Board of Education of Decatur Public School District No. 61, 478 N.E.2d 1209 (Ill.App.4, 1985). Nevertheless, before access privileges are revoked, the user should be allowed to give an explanation.

[9] If students are allowed only supervised access and are not required to sign the *Authorization for Electronic Network Access*, the provisions from the *Authorization* should be used as administrative procedures for covering student Internet use. See *Acceptable Use of Electronic Networks*, 6:235-AP. This is an optional sentence:

> [9] The Superintendent shall establish administrative procedures containing the appropriate uses, ethics, and protocol for Internet use.

[9] The Harassing and Obscene Communications Act criminalizes harassing and obscene electronic communication (720 ILCS 135/0.01).

[10] The Fourth Amendment protects individuals from searches only when the person has a legitimate expectation of privacy. This provision attempts to avoid Fourth Amendment protection for communications and downloaded material by forewarning users that their material may be read or searched, thus negating any expectation of privacy.

[10] Email and computer files are "public records" as defined in the Ill. Freedom of Information Act if they are, as in this policy, "under control" of the school board (5 ILCS 140/2). They may be exempt from disclosure, however, when they contain information that, if disclosed, "would constitute a clearly unwarranted invasion of personal privacy," (5 ILCS 140/7). Alternatively, a school board may believe that making email semi-private enhances its educational value. The following grants limited privacy to email communications and can be substituted for the sample policy's sentence preceding this footnote:

> [10] School officials will not intentionally inspect the contents of email without the consent of the sender or an intended recipient, unless as required to investigate complaints regarding email that are alleged to contain material in violation of this policy or the *Authorization for Electronic Network Access*.

[11] Supra f/n #1.

[12] This sample policy language is broader than the requirements in federal law (20 U.S.C. §6777, 47 U.S.C. §254, and 47 C.F.R. §54.520(c)(i). It does not distinguish between minors (children younger than 17) and non-minors. The terms, *minor*, *obscene*, *child pornography*, and *harmful to minors* have not changed, but are now explicitly referred to in the regulations at 47 C.F.R. §54.520(a). Federal law defines *harmful to minors* as:

> [12] …any picture, image, graphic image file, or other visual depiction that–(i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. [13] The Superintendent or designee shall include measures in this policy's implementation plan to address the following: [14]

1. Ensure staff supervision of student access to online electronic networks, [15]
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access [16]

Each staff member must sign the District's *Authorization for Electronic Network Access* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use. [17]

All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network.

---

[12] The Federal Communications Commission specifically declined to find that access to *Facebook* or *MySpace* are per se *harmful to minors*. School officials have discretion about whether or not to block access to these and similar sites. See supra f/n #3.

[13] Permitted by 20 U.S.C. §6777(c). The policy's provision for prior approval is not in the law and may be omitted. The entire sentence may be eliminated if a board does not want the filtering device to be disabled.

[14] In order to qualify for universal service benefits under the federal Children's Internet Protection Act (CIPA), the district's Internet safety policy must address the items listed in the sample policy (47 U.S.C. §254(l). The sample policy accomplishes this task by requiring these items be addressed in the policy's implementation plan or administrative procedure.

[14] Note that federal law requires the school board to hold at least one hearing or meeting to address the *initial* adoption of the Internet safety policy. Later revisions of the existing policy need not follow the public notice rule of CIPA, though a board will still need to follow its policy regarding revisions and the mandates of the Ill. Freedom of Information Act.

[14] CIPA also requires this policy and its documentation to be retained for at least 5 years after the last day of service delivered in a particular funding year. This means the 5 year retention requirement begins on the last day of service delivered under E-rate not from the day the policy was initially adopted. Consult the board attorney about this requirement and the best practices for your individual board.

[15] Monitoring the online activities of *students* is broader than the requirement in federal law to monitor *minors*. The definition of minor for this purpose is "any individual who has not attained the age of 17 years." See 47 C.F.R. 54.520(a)(4)(i). The use of the word *students* is a best practice.

[16] The *Authorization for Electronic Network Access* (6:235-E2), rather than this board policy, specifies appropriate conduct, ethics, and protocol for Internet use. This is consistent with the principle that detailed requirements are not appropriate for board policy; instead, they should be contained in separate district documents that are authorized by board policy. Keeping technical rules specifying acceptable use out of board policy will allow for greater flexibility, fewer changes to the policy manual, and adherence to the belief that board policy should be confined to governance issues and the provision of guidance on significant district issues.

[17] The Superintendent's implementation plan should describe appropriate supervision for students on the Internet who are not required, or refuse, to sign the *Authorization*.

[17] The use of personal electronic communication devices owned by students but used to gain Internet access that has been funded by *E-rate* is not addressed yet. The FCC has indicated that it does plan to address the issues associated with the application of CIPA requirements to this situation.

The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).
Enhancing Education Through Technology Act, 20 U.S.C §6751 et seq.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications)

ADMIN PROC.: 6:235-AP1 (Administrative Procedure - Acceptable Use of Electronic Networks), 6:235-AP1, E1 (Student Authorization for Electronic Network Access), 6:235-AP1, E2 (Exhibit - Staff Authorization for Electronic Network Access)