Instruction

Access to Electronic Networks [1]

Electronic networks are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. [2]

The term *electronic networks* includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-issued Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networks or to any District-issued online account from any computer or device, regardless of location;
3. District-owned or District-issued computers, laptops, tablets, phones, or similar devices.

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

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[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.

A policy on Internet safety is necessary to receive *E-rate* funds under the Elementary and Secondary Education Act, Student Support and Academic Enrichment Grants (20 U.S.C. §7131) and to qualify for universal service benefits under the Children's Internet Protection Act (CIPA) (47 U.S.C. §254(h) and (l)).

Generally, federal rules prohibit schools from soliciting or accepting gifts or other things of value exceeding $20 from Internet service providers that participate or are seeking to participate in the E-rate program. 47 C.F.R. §54.503. However, during the COVID-19 pandemic, the Federal Communications Commission (FCC) temporarily waived its rules prohibiting such gifts to enable service providers to support remote learning efforts without impacting school E-rate funding. See https://docs.fcc.gov/public/attachments/DA-20-1479A1.pdf.

[2] This goal is repeated in sample exhibits 6:235-AP1, E1, *Student Authorization for Access to the District's Electronic Networks*, and 6:235-AP1, E2, *Staff Authorization for Access to the District's Electronic Networks*.

[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 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.

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) cyberbullying 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]

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] Users of the District's electronic networks have no expectation of privacy in any material that is stored on, transmitted, or received via the District's electronic networks. General rules for behavior and communications apply when using electronic networks. The District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, contains the appropriate uses, ethics,

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[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. All boards receiving an *E-rate* funding for Internet access were required to certify that they had updated their Internet safety policies. See, *FCC Report and Order 11-125* (8-11-11). 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 Sch. Dist. v. Kuhlmeier, 484 U.S. 260 (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.

It is an unfair labor practice (ULP) under the Ill. Educational Labor Relations Act (IELRA) for an employer to discourage employees from becoming or remaining members of a union. 115 ILCS 5/14(a)(10). In connection with that potential penalty, the IELRA requires employers to establish email policies in an effort to prohibit the use of its email system by outside sources. 115 ILCS 5/14(c-5). This policy aligns with IELRA requirements by clarifying the District's electronic network is not a public forum for general use by outside parties and by limiting use of the network to the purposes stated under the **Acceptable Use** subhead. However, districts are still prohibited under the First Amendment to the U.S. Constitution from suppressing messages based on viewpoint and may be subject to liability if they affirmatively block individual senders. See Lindke v. Freed, 601 U.S. 187 (2024); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37 (1983); People for the Ethical Treatment of Animals v. Tabak, 109 F.4th 627 (D.C. Cir. 2024). Consult the board attorney if the board wants to amend this policy to prohibit access by specific parties and/or before taking steps to "block" any specific party from the district's email system based on the content of the party's message.

[7] This paragraph provides general guidelines for acceptable use regardless of whether Internet use is supervised. In practice, many districts allow for incidental personal use of their networks during duty-free times. The specific rules are provided in sample exhibits 6:235-AP1, E1, *Student Authorization for Access to the District's Electronic Networks,* and 6:235-AP1, E2, *Staff Authorization for Access to the District's Electronic Networks* (see also f/n 1). 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. Bd. of Educ. of Decatur Public Sch. Dist. No. 61, 133 Ill.App.3d 531 (4th Dist. 1985). Nevertheless, before access privileges are revoked, the user should be notified and allowed to give an explanation.

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.[12] 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.[13] The Superintendent or 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.[14] The

---

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[9] If students are allowed only supervised access and are not required to sign the *Authorization for Access to the District's Electronic Networks*, the provisions from the *Authorization* should be used as administrative procedures for covering student Internet use. See 6:235-AP1, *Acceptable Use of the District's Electronic Networks*. This is an optional sentence:

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

The Harassing and Obscene Communications Act criminalizes harassing and obscene electronic communication. 720 ILCS 5/26.5.

[10] The Fourth Amendment to the U.S. Constitution 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.

Email and computer files are "public records" as defined in the Ill. Freedom of Information Act (FOIA) 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:

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 is alleged to contain material in violation of this policy or the District's administrative procedure, *Acceptable Use of the District's Electronic Networks*.

[11] See f/n 1.

[12] While it is best practice to do so, neither CIPA nor the rules for the E-Rate program specifically address whether school-owned computers or other mobile computing devices must be filtered when using a non-school Internet connection. Consult the board attorney for guidance on this issue.

[13] This sample policy language is broader than the requirements in federal law (20 U.S.C. §7131, 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:

…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.

The Federal Communications Commission specifically declined to find that access to social networking websites are per se *harmful to minors*. However, the U.S. Dept. of Health and Human Services issued a Surgeon General's Advisory stating there is not enough evidence to conclude that social media is safe for children. See www.hhs.gov/surgeongeneral/reports-and-publications/youth-mental-health/social-media/index.html. School officials have discretion about whether or not to block access to these and similar sites. See supra f/n 3.

[14] Permitted by 20 U.S.C. §7131(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.

Superintendent or designee shall include measures in this policy's implementation plan to address the following: [15]

1. Ensure staff supervision of student access to online electronic networks, [16]
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.

Use of Artificial Intelligence (AI)-Enabled Tools [17]

The Board recognizes that AI-enabled tools are important to enhance student learning, educator effectiveness, and school operations. The use of AI-enabled tools in the District shall be implemented in a safe, ethical, and equitable manner and in accordance with Board policies 1:30, *School District Philosophy*, and 7:345, *Use of Educational Technologies; Student Data Privacy and Security.*

To implement the use of AI-enabled tools in the District, the Superintendent or designee shall:

1. Develop a District-wide AI Plan that addresses the District's approach to the integration of AI;
2. Based on the District-wide AI Plan, establish AI Responsible Use Guidelines to address the responsible use of AI in the District by students and staff;

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[15] 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.

Note that federal law required school boards 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 FOIA.

CIPA also requires this policy and its documentation to be retained for at least five years after the last day of service delivered in a particular funding year. This means the five-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.

[16] 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.

[17] Optional. Artificial intelligence is a rapidly evolving and complex technology that implicates many unsettled legal and ethical issues. This content 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.

A Statewide Generative AI and Natural Language Processing Taskforce issued a report to the General Assembly in December 2024 (https://doit.illinois.gov/content/dam/soi/en/web/doit/meetings/ai-taskforce/reports/2024-gen-ai-task-force-report.pdf) that recommended the Ill. State Board of Education provide guidance on the use of AI in schools, best practices, and educator training. The U.S. Dept. of Education released a toolkit to assist education leaders with the safe, ethical, and equitable integration of AI within education systems, available at: http://downloads.microscribepub.com/il/press/federal_resources/FINAL-ED-OET-EdLeaders-AI-Toolkit-10.29.24_20250221.pdf. Note: This resource may no longer be available on a federal government website but is being maintained at **PRESS** Online to provide consistent subscriber access.

Adopting policy language that addresses AI provides (a) a way for boards to monitor how this technology is being used in the district, and (b) an opportunity for the board and the superintendent to examine all current policies, collective bargaining agreements, and administrative procedures on this subject. Before adoption of this subhead, the board may want to have a conversation with the superintendent to determine how local conditions, resources, and current practices will support the full implementation of a policy that addresses AI and its goals. The use of AI will be most effective when the policy reflects local conditions and circumstances. Consult the board attorney about these issues. See sample administrative procedure 6:235-AP3, *Development of Artificial Intelligence (AI) Plan and AI Responsible Use Guidelines*, for a suggested framework for developing an AI plan and guidelines.

3. Ensure that AI-enabled tools comply with State and federal law;
4. Ensure that staff receive training and students receive instruction on the use of AI, as appropriate; and
5. Review the District's AI Plan and AI Responsible Use Guidelines on an annual basis and update them as needed.

Authorization for Electronic Network Access [18]

Each staff member must sign the *Authorization for Access to the District's Electronic Networks* 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. [19]

Confidentiality

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.

Violations

The failure of any user to follow the terms of the District's administrative procedure, *Acceptable Use of the District's Electronic Networks*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

The footnotes are not intended to be part of the adopted policy; they should be removed before the policy is adopted.

[18] The District's administrative procedure, 6:235-AP1, *Acceptable Use of the District's Electronic Networks*, 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. This sample policy only requires staff and students to sign the *Authorization*; however, all users of the District's Electronic Networks, including board members and volunteers, are bound by this policy and its implementing procedure and should be familiar with their content.

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

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.

LEGAL REF.: 20 U.S.C. §7131, Elementary and Secondary Education Act.
47 U.S.C. §254(h) and (l), Children's Internet Protection Act.
47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.
115 ILCS 5/14(c-5), Ill. Educational Labor Relations Act.
720 ILCS 5/26.5.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40 (Curriculum Development), 6:60 (Curriculum Content), 6:210 (Instructional Materials), 6:220 (Bring Your Own Technology (BYOT) Program; Responsible Use and Conduct), 6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools), 7:315 (Restrictions on Publications; High Schools), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

ADMIN. PROC.: 6:235-AP1 (Acceptable Use of the District's Electronic Networks), 6:235-AP1, E1 (Student Authorization for Access to the District's Electronic Networks), 6:235-AP1, E2 (Staff Authorization for Access to the District's Electronic Networks)