PRESS PLUS ISSUE #123 (OCTOBER 2026)
11/13/26 POLICY COMMITTEE MEETING

1. **ACTION TO BE TAKEN:**

_____CONSENT

_____1st READING

_____KEEP IN COMMITTEE

_____DELETE POLICY

2. **POLICY COMMITTEE TO DETERMINE:**

___ Adopt as Presented
(change "revised" & "reviewed" date)

___Adopt with Additional District Edits
(change "revised" & "reviewed" date)

___Edits Not Adopted
(change "reviewed" date)

Document Status: Draft Update

SECTION 6 - Instruction

6:235 Access to Electronic Networks

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.

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

Updated in response to the expanded use of educational technologies in schools and for other continuous improvements. **Issue 107, June 2021**

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 or designee shall develop an implementation plan for this policy. Each Building Principal shall act as the "system administrator" for his or her building.

The School District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. 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) cyberbullying awareness and response. 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.

Acceptable Use

All use of the District's electronic network must be (1) in support of education and/or research, and be in furtherance of the Board of Education's stated goal, or (2) for a legitimate school business purpose. Use is a privilege, not a right. 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 or District computers. 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, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

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 the Children's Internet Protection Act and as determined by the Superintendent or designee. 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.

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

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

Mobile Devices

The Board has authorized a system of mobile devices, in which each student is issued a District device for use as part of the curriculum. The use of mobile devices will be governed by administrative procedures and/or guidelines established by the Superintendent or designee or by a handbook approved by the Superintendent or designee, which at a minimum must:

1. Require that students and parents sign a separate authorization before being issued a device.
2. Ensure that all devices have Internet content filtered by the District and may be monitored remotely for inappropriate use.
3. Clearly spell out parents’ financial responsibility in the event of loss of or damage to a device.

Prohibited Conduct When Using the District Computer Network

1. Students may be subject to discipline, including, but not limited to, suspension, expulsion or loss of network privileges, for the following conduct:
    1. Invading the privacy of individuals, including, but not limited to, the unauthorized release of any student’s or school staff’s personal identifying information (such as personal addresses or telephone numbers).
    2. Using the Internet in any way that is not reasonably related to the Lincolnwood School District’s educational goals and objectives. This includes, but is not limited to:
        1. Chain Letters. Spam, and other unsolicited, non-educational communication.
        2. Unauthorized intentional downloads to a single computer, network drive or external storage media, of movies or video files (unless specifically assigned); MP3s; shareware; freeware; pirated software; or other .exe or application files.
        3. Registration to receive email communications or services for anyone other than the originating user from listserves or other free subscription services for anyone other than the originating user.
        4. Participation in non-district posted message boards or social media sites, chat rooms or sites, including but not limited to, Facebook,

Instagram, TikTok, Twitch, Reddit, Discord, Yahoo! Messenger or Yahoo! Chat, MIRC, ICQ, AOL Instant Messenger. MSN Messenger, myspace.com, and facebook.com.

3. Viewing, sending or displaying offensive messages or pictures.
4. Viewing, sending or displaying sexually explicit messages or media.
5. Viewing, sending or displaying obscene language.
6. Harassing, insulting, or attacking others.
7. Damaging or attempting to damage computers, computer systems, computer networks, hardware, or software.
8. Violating copyright laws.
9. Using another's password.
10. Trespassing in another's folder, work, or files.
11. Employing the network for commercial purposes.
12. Posting anonymous messages without a legitimate educational purpose.
13. Any behavior that causes a material disruption to the educational environment.

2. In addition to disciplinary consequences, legal action may be taken where appropriate.

Use of Artificial Intelligence (AI)-Enabled Tools[C1]

The Board recognizes that evidence-based technology tools that use AI (AI-enabled tools) have the potential 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 compliance with applicable federal and State laws. The use of AI-enabled tools shall be in accordance with Board policies, including, but not limited to, 7:340, *Student Records,* and 7:345, *Use of Educational Technologies; Student Data Privacy and Security.* Any staff use of AI-enabled tools will not replace educator judgment, human relationships, or adult accountability. Any student use of AI-enabled tools shall support and strengthen, rather than replace or diminish, students' critical thinking and agency.

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;[C2]
2. Based on the District-wide AI Plan, establish AI Responsible Use Guidelines to

address the informed and responsible use of AI in the District by students and staff;
3. Ensure that any AI-enabled tools used in the District have been properly vetted for safety, security, and operational and instructional fit, as applicable, and compliance with this policy;[C3]
4. Maintain a list of District-approved AI-enabled tools that is accessible to staff, students, and parents/guardians, as appropriate;[C4]
5. Ensure that staff receive regular training on AI use and students receive developmentally appropriate AI literacy instruction, as appropriate;[C5]
6. Review the District's AI Plan and AI Responsible Use Guidelines on an annual basis and report any necessary updates to the Board;[C6] and
7. Annually report to the Board on the impact of the use of AI-enabled tools on teacher effectiveness and student outcomes in the District, as applicable.[C7]

Authorization for Electronic Network Access

Each staff member must sign the District's *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.

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 student or staff member 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.

LEGAL REF.:

20 U.S.C. §1232g, Family Educational Rights and Privacy Act.

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.

105 ILCS 10/, Ill. School Student Records Act.

105 ILCS 85/, Student Online Personal Protection Act.

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), 6:230 (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), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

ADOPTED: September 10, 2002

REVISED: June 26, 2025

REVIEWED: June 26, 2025

Lincolnwood School District 74

PRESSPlus Comments

C1.

The Use of Artificial Intelligence (AI)-Enabled Tools subhead is rewritten for PRESS Plus. A redlined version showing the changes made is available at PRESS Online by logging in at www.iasb.com. Please also compare this new text with the policy language previously adopted by the Board.

This entire subhead is optional, and it may be modified at the Board's discretion. For more information, see the footnotes available at PRESS Online by logging in at www.iasb.com.

The subhead is updated in response to the Ill. State Board of Education's (ISBE) nonregulatory *Statewide Guidance on the Use of Artificial Intelligence* (June 2026), available at www.isbe.net/Pages/AI-Guidance.aspx. In accordance with 105 ILCS 5/2-3.118a, added by P.A. 104-399, the Guidance addresses AI in pre-K through 12 education. The Guidance emphasizes the need for schools to reflect on local values, context, and priorities as they consider AI use. It relies on four main principles: (1) teaching and learning are shaped by relationships and by the experiences, interests, and assets each child brings to school; (2) schools serve academic, developmental and civic purposes concurrently; (3) AI is a means to inform teaching and learning rather than an end in itself; and (4) informed use (of AI) requires deliberate, context-sensitive, and *locally determined* purpose and use (emphasis added). The Guidance states the central question around AI use in schools is not whether a tool can simply perform a task, "but whether its use supports the purposes of schooling: the growth of the individual, the strengthening of human relationships, the exercise of judgment and responsibility, and preparation for thoughtful participation in a world increasingly shaped by digital and AI-mediated environments."

The U.S. Dept. of Education also issued a *Dear Colleague Letter* on 8-20-26, to help school districts make informed decisions about the responsible use of technology in classrooms, at: www.ed.gov/media/document/guidance-education-technology-and-screentime-schools-114386.pdf.

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. For suggested board monitoring questions around a district's use of AI, please see sample policy 6:235's footnote 17, available at PRESS Online by logging in at www.iasb.com.

Issue 123, October 2026

C2. If a board wishes to exercise greater oversight over the AI Plan, add the following to the end of this item: ", which shall be approved by the Board". If adding edits, use the Save Status **Adopted with Additional District Edits**. **Issue 123, October 2026**

C3. ISBE's Guidance (www.isbe.net/Pages/AI-Guidance.aspx, p. 103), recommends that AI applications be vetted for operational and instructional fit using clear questions tied to purpose and use. **Issue 123, October 2026**

C4. ISBE's Guidance (www.isbe.net/Pages/AI-Guidance.aspx, p. 10) recommends that districts maintain clear information about approved tools, their purpose and use, data security, and contact points for questions or concerns. **Issue 123, October 2026**

C5. ISBE's Guidance (www.isbe.net/Pages/AI-Guidance.aspx, p. 226) states that students should learn about AI, including what it is (and is not), how it works, its impact on society, and how to shape it, *before* and while using AI tools in the classroom. **Issue 123, October 2026**

C6. A board can modify the review schedule as desired. Federal guidance recommends that educational leaders establish the cadence in which the learning community will review and update the responsible use policy (guidelines) based on use, technological updates, and feedback. See https://downloads.microscribepub.com/il/press/federal_resources/FINAL-ED-OET-EdLeaders-AI-Toolkit-10.29.24_20250221.pdf, p. 52. ISBE Guidance also recommends "periodic review," see www.isbe.net/Documents/AIGuidance.pdf, p. 176. **Issue 123, October 2026**

C7. A board can modify the reporting schedule as desired. ISBE Guidance emphasizes the importance of having clarity on whether AI use is improving practice and/or student outcomes. See https://www.isbe.net/Documents/AIGuidance.pdf, pp. 111, 141, 227, and 229. **Issue 123, October 2026**