SECTION 6 - INSTRUCTION

6:235 Access to Electronic Networks

Redline against the PRESS Issue 123 Draft Update of Lisle's 6:235 (packet pages 78-84). ~~Struck red text with blue highlight~~ is removed from the PRESS draft. Underlined red text with blue highlight is added by Lisle. Unmarked text is unchanged from the PRESS draft, including the AI subhead IASB rewrote in Issue 123.

Electronic ~~networks*~~ networks 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:

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.~~ devices; and
4. Artificial intelligence (AI)-enabled tools that the District provides, licenses, or approves for student or staff use, including AI features within other District-approved software.

The Superintendent or designee shall develop an implementation plan for this policy and appoint a system administrator.

The District is not responsible for any losses or damages incurred 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;~~ 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 networks are part of the curriculum and are not public forums for general use.

~~Acceptable~~ Responsible Use

All use of the District's electronic networks must be:

1. In support of education and/or research, and be in furtherance of the School Board's stated goal, or

2. For a legitimate school business purpose.

~~*Electronic Networks include, but are not limited to:~~

1. ~~The Internet~~
2. ~~Any wireless access~~
3. ~~Internet access~~
4. ~~Remote access to District internal network~~

Use is a privilege, not a right. General rules for behavior and communications apply when using electronic networks. The District's ~~Acceptable Use Standards (AUS)~~ administrative procedure 6:235-AP1, Responsible Use of the District's Electronic Networks, contains the appropriate uses, ethics, and protocol. 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. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

School officials may conduct an investigation or require a student to cooperate in an investigation if there is specific information about the activity on the student's phone or account on a social networking website that violates a school disciplinary rule or policy. In the course of the investigation, the student may be required to share the content that is reported in order to allow school officials to make a factual determination.

~~All users of the District's computers and means of Internet access 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.~~

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

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including "hacking" and other unlawful ~~activities:~~ activities; and

4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Use of Artificial Intelligence (AI)-Enabled Tools

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.

AI-enabled tools shall not be the sole basis for any decision that significantly affects a student or employee, including grading, discipline, placement, special education or Section 504 eligibility and services, and employment decisions. Such decisions require documented review by an appropriate staff member.

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 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;~~ policy, including a written agreement that complies with the Student Online Personal Protection Act before any AI-enabled tool receives student data;
4. Maintain a list of District-approved AI-enabled tools that is accessible to staff, students, and parents/guardians, as appropriate;
5. Ensure that staff receive regular training on AI use and students receive developmentally appropriate AI literacy instruction, as appropriate; and
6. Review the District's AI Plan and AI Responsible Use Guidelines on an annual basis ~~and report any necessary updates to the Board; and~~ and, as part of the annual School Improvement presentations to the Board, report any necessary updates and the District's observations, available data, and lessons learned regarding the use of AI-enabled tools, including AI features within other District educational technologies, in relation to teacher effectiveness and student outcomes, as applicable.
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.~~

Authorization for Electronic Networks Access

Each staff member must sign the ~~District's Acceptable Use Standards (AUS)~~ Staff Authorization for Responsible Use of the District's Electronic Networks (6:235-AP1, E2) as a condition for using the District's electronic networks. Each student and his or her ~~parent(s)/guardians(s)~~

parent(s)/guardian(s) must sign the ~~AUS~~ Student Authorization for Responsible Use of the District's Electronic Networks (6:235-AP1, E1) before being granted ~~supervised~~ unsupervised use.

~~The failure of any student or staff member to follow the terms of the Acceptable Use Standards, or this Board policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.~~

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.~~ network or entered into any AI-enabled tool.

Violations

The failure of any user to follow the terms of the District's administrative ~~procedure, Acceptable~~ procedure 6:235-AP1, Responsible Use of the District's Electronic Networks, the District's AI Responsible Use Guidelines, 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 5/2-3.118a, Statewide guidance on artificial intelligence.

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 Resource Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:15 (Student and Family Privacy Rights), 7:130 (Student Rights and Responsibilities), 7:180 (Prevention of and Response to Bullying, Intimidation, and Harassment), 7:190 (Student Behavior), 7:310 (Restrictions on Publications; Elementary Schools), 7:315 (Restrictions on Publications; High Schools), 7:340 (Student Records), 7:345 (Use of Educational Technologies; Student Data Privacy and Security)

ADOPTED: July 27, 2026

REVISED: [DATE]