Access to Electronic Networks and Instructional Technology

Electronic networks and instructional technology, 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 District's *electronic networks and instructional technology* 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 other 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 a system administrator(s).

The District is not responsible for any information that may be lost or damaged, or become unavailable when using the District's electronic networks and instructional technology, 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 District's electronic networks and instructional technology 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 and instructional technology are part of the curriculum and are not a public forum for general use.

Acceptable Use

All use of the District's electronic networks and instructional technology 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. Students and staff members have no expectation of privacy in any material that is stored on, transmitted, or received via the District's electronic networks or instructional technology. General rules for behavior and communications apply when using electronic networks and instructional technology. The District's Administrative Procedure, *Acceptable Use of the District's Electronic Networks and Instructional Technology,* 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.

Adopted: May 28, 1997
Reviewed: May 2026
Amended: June 17, 2026

Internet Safety

Technology protection measures shall be used on each District computer or device 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. 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 received 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 personally identifiable information, such as, names and addresses.

Use of Artificial Intelligence (AI)-Enabled Tools

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, *District Mission Statement, Vision Statement, and Commitments*, and 7.345, *Operator Use of 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;
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 Networks and Instructional Technology Access

Each student and staff member must agree to the *Authorization for Access to the District's Electronic Networks and Instructional Technology* as a condition for using the District's electronic networks and instructional technology.

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 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 and Instructional Technology*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

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), 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 (Operator Use of Student Data; Privacy and Security)

ADMIN.PROC.: 6.235-AP1 (Acceptable Use of the District's Electronic Networks and Instructional Technology), 6.235-AP1, E1 (Student Authorization for Access to the District's Electronic Networks and Instructional Technology), 6.235-AP1, E2 (Staff Authorization for Access to the District's Electronic Networks and Instructional Technology)

Adopted: May 28, 1997
Reviewed: May 2026
Amended: June 17, 2026