

## Instruction

### Access to Electronic Networks

Electronic networks are a part of the District's instructional program in order 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 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 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 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 Executive Board's stated goals, and (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 network. 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, 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 federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. 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.

Authorization for Electronic Network Access

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.

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.

- 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.  
 115ILCS 5/14(c-5), Ill. Educational Labor Relations Act.  
 720 ILCS 135/0.01.
- CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright for Publication or Sale of Instructional Materials and Computer Programs Developed by Employees), 6:40 (Curriculum Development), 6:210 (Instructional Materials), 6:230 (Library Resource Center), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Publications); 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)
- ADOPTED: September 23, 2004
- REVIEWED: July 23, 2020; October 28, 2021
- REVISED: December 20, 2007; September 27, 2012; September 22, 2016; October 28, 2021