6:235 Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program. The Superintendent or designee shall develop an implementation plan for this policy and designate system administrator(s) for use of computer network systems including the Internet.

For the purposes of this policy and its accompanying procedures, individual School Board members and administrative staff members shall be treated like teachers and the term electronic network shall include all information accessed by Internet sites, E-Mail, on-line services, bulletin board systems and local services.

The electronic network is part of the District's curriculum and is not a public forum for general use. Consequently, the network may be used solely for educational purposes and school-related business and functions. When used as part of the curriculum, the electronic network shall (1) be directly related to 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-media 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) cyber-bullying awareness and response.

All network users must 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. Staff and students have no expectation of privacy in their use of the District's network. Electronic communications and downloaded material may be monitored or read by school officials.

No Expectation of Privacy

All information or files created, placed, transmitted, or received through the District's computer network may be opened, reviewed, copied and used by school officials and/their designees at any time they deem appropriate in connection with the protection of the network, the application or enforcement of any school policy or suspected violations of the law. There are no expectations of privacy with respect to any such information or documents, except as may be provided by applicable law governing the privacy of student records and information.

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. 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. Use safeguards to protect 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.

Each staff member must sign and agree to abide by the District's Authorization for Electronic Network Access as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must also sign and agree to abide by the Authorization before being granted unsupervised use.

The failure of any student or staff member to follow the terms of the Authorization for Electronic Network Access, this policy, or its accompanying procedures will result in the loss of privileges, disciplinary action, up to and including discharge in the case of staff, and suspension and/or expulsion in the case of students. Illegal use of the District's computers will result in referral to law enforcement agencies.

LEGAL REF.:

No Child Left Behind Act, 20 U.S.C. §6777.

Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).

Enhancing Education Through Technology Act, 20 U.S.C §6751 *et seq.*

47 C.F.R. Part 54, Subpart F, Universal Service Support for Schools and Libraries.

720 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 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 (Restrictions on Publications)

ADOPTED: September 24, 2012