New Press Plus Issue #107/June 2021 for 7/23/21 Policy Committee

Document Status: Draft Update

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:[PRESSPlus1]

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. ~~Students and staff members~~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.

Prohibited Conduct When Using the District Computer Network

A. 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:
        a. Chain Letters.
        b. 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.
        c. Registration to receive email from listserves or other free subscription services for anyone other than the originating user.
        d. Participation in non-district posted chat rooms or sites, including but not limited to, Yahoo! Messenger or Yahoo! Chat, MIRC, ICQ, AOL Instant Messenger. MSN Messenger, myspace.com, facebook.com.:
    3. Viewing, sending or displaying offensive messages or pictures.
    4. Viewing, sending or displaying sexually explicit messages or pictures.
    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.
    13. Any behavior that causes a material disruption to the educational environment.
B. In addition to disciplinary consequences, legal action may be taken where appropriate.

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[PRESSPlus2] 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.:

~~No Child Left Behind Act, 20 U.S.C. §6777~~ 20 U.S.C. §7131, Elementary and Secondary Education Act.

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

~~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.

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: September 6, 2012

REVIEWED: September 6, 2012

PRESSPlus Comments

PRESSPlus 1. Updated in response to the expanded use of educational technologies in schools and for other continuous improvements. **Issue 107, June 2021**

PRESSPlus 2. This policy only requires staff and students to sign the *Authorization;* however, all users of the District's Electronic Networks, including board members and volunteers, are bound by this policy and its implementing procedure and should be familiar with their content. The District's administrative procedure, 6:235-AP1, *Acceptable Use of the District's Electronic Networks* (available at PRESS Online by logging in at www.iasb.com), rather than this board policy, specifies appropriate conduct, ethics, and protocol for Internet use. **Issue 107, June 2021**