Instruction

Access to Electronic Networks

Electronic networksare 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.

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

The District is not responsible for any information that may be lost, or damaged, or become 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-media center materials. As required by federal law, *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. 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's stated goal, or (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*, *Access* 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.

Unacceptable Uses

The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

a. Activities which interfere with the ability of others to use the network;
b. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law;
c. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
d. Downloading copyrighted material for other than personal use;
e. Using the network for private financial or commercial gain;
f. Wastefully using resources, such as file space;
g. Hacking or gaining unauthorized access to files, resources, or entities;
h. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;
i. Using another user's account or password;
j. Posting material authorized or created by another without his/her consent;
k. Posting anonymous messages;
l. Using the network for commercial or private advertising;
m. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
n. Using the network while access privileges are suspended or revoked.
o. Engaging in cyber bullying.

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 while at school,
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.

User Training

Each person using the District network will be expected to complete training successfully before being allowed access. This training will include, but is not necessarily limited to, login and logoff procedures, e-mail, list serves, world wide web, vandalism, viruses, copyright laws, and internet etiquette.

Privilege Suspension

Anyone who is found in violation of the acceptable use standards for the District network or *the Authorization for Electronic Network Access* may have their network privileges canceled. A review by the administration after a period of time may be requested.

Accountability

If the District incurs costs because a user engages in unauthorized "electronic commerce" (despite the same being a violation of the network use standards), such user will be responsible for reimbursing the District for such costs.

Authorization for Electronic Network Access

Each staff member will receive the *Staff Authorization for Access to the District's Electronic*. Each parent/guardian will receive the *Student Authorization for Access* to the *District's Electronic Networks* through then online registration process and via the parent-student handbook.

Confidentiality

All users of the District's computers with access to 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 *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.
115 ILCS 5/14(c-5), Ill. Educational Labor Relations Act.
720 ILCS 135/0.01.

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; Responsible Use and Conduct).6:230 (Library Media Program), 6:260 (Complaints About Curriculum, Instructional Materials, and Programs), 7:130 (Student Rights and Responsibilities), 7:190 (Student Discipline), 7:310 (Restrictions on Publications; Elementary Schools) 7:345 (Use of Educational Technologies; Student Data Privacy ad Security)

ADMIN PROC.: 6:235-AP1 (Acceptable Use of Electronic Networks), 6:235-APE1 (Student Authorization for Electronic Network Access), 6:235-AP1, E2 (Staff Authorization for Electronic Network Access).

ADOPTED: December 11, 2007

REVISED: February 26, 2013

October 25, 2016

November 23, 2021