INSTRUCTION

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

The School 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 network 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 Media/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) 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 networks 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, 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 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. 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 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.

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.

The failure of any student or staff member 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.

Website
The District 67 Website is a closed forum. It shall be used for District purposes to transmit information to the public.

Copyright
The policy should contain a rule against illegal publication or copying of copyrighted material, and a statement that employees will be held personally liable for any of their own actions that violate copyright laws.

Harassment
School policies against sexual harassment and other forms of discriminatory harassment apply equally to communication on school computer systems.

Misuse of networks, hardware or software
Damage caused by intentional misuse of equipment will be charged to the user.

Safeguard account and passwords
Employees are responsible for safeguarding their own passwords, and they will be held accountable for the consequences of intentional or negligent disclosure of this information.

Illegal uses
Illegal use shall not be permitted.

Advertising
Advertising and solicitation by employees for personal business is prohibited on school computers. Employees are also prohibited from sending personal messages from a home or other outside computer to school district e-mail users.

Fundraising, non-profit or charitable solicitation
Charitable solicitation and/or advertising for not-for-profit agencies is prohibited unless the event is school/district sponsored.

Representing personal views as those of the school district
Any e-mail sent from the school computer is likely to contain a return address identifying the school district. Thus, sending an e-mail from the school is analogous to an employee using school letterhead. Accordingly, employees should be careful not to have their own statements mistakenly attributed to the district.

Downloading or loading software or applications without permission from the administrator
There is an enormous quantity and variety of free software available on the Internet. In addition to viruses that could infect the school's systems, the cumulative effect of widespread downloading on the school's computers, in terms of degradation of performance and additional maintenance, can be significant. Use or downloading of outside software requires pre-approval from the technology coordinator or system administrator.

The Federal Family Educational Rights and Privacy Act restricts disclosure of personally identifiable information from a student's "educational records." An e-mail message itself may well constitute an "education record" which should be protected under the law. When a staff member communicates with another staff member concerning a student for legitimate educational purposes, that kind of information-sharing is not prohibited by FERPA. Disclosures about students to staff members who have no need for the information or especially to outside persons, could violate FERPA and is therefore prohibited.

It shall be the responsibility of the director of technology to maintain a filtering system which is current and effective.

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), 6:60 (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)

ADMIN PROC.: 6:235-AP1 (Administrative Procedure - 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 (Exhibit - Staff Authorization for Access to the District's Electronic Networks)

ADOPTED: September 16, 1999

REVIEWED: November 15, 2012; January 21, 2016

REVISED: August 16, 2001; April 1, 2003, August 25, 2016; February 16, 2017