

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional and operational environment, which serves to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent 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, 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.

The same policies and procedures apply to Board members and administrative staff members as apply to teachers or other individuals granted access to District electronic networks. "Internet" includes, but is not limited to, all information accessed by Internet sites, District websites, email, on-line services, social networking, blogging, tweeting and bulletin board systems.

Curriculum

The use of District's electronic networks shall:

- 1) be consistent with curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities and developmental levels of the student; and
- 2) comply with the selection criteria for instructional materials and library resource materials. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum. Users shall consider the impact of Internet bandwidth of District electronic networks by contacting the system administrator(s) before utilizing video streaming, audio streaming or remotely connecting to other users outside of the District's electronic networks.

The District's electronic networks are part of the curriculum and are not to be considered as a public forum for general use. Those users that do not use the Internet within the curriculum should limit use of the Internet to specific areas of operational use that pertain to job functionality. Inadvertent or personal use of the Internet should be limited and not interfere with a user's job duties as assigned.

District resources, such as laptops and cell phones, provided to staff members for curricular and/or operational job functions are the property of the District and should not be viewed as personal equipment, even when authorized to use the equipment outside of school hours.

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 Board's stated goals, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Users of the District electronic networks have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. The District's *Acceptable Use of Electronic Networks* procedure contains appropriate uses, ethics and protocols for users to follow. 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

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate 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(s).

The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Excessive personal use that contradicts the educational goals of the District.
2. Unauthorized bandwidth usage that is deemed detrimental to overall network performance.
3. Unauthorized access, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each user must accept the terms of the *Electronic Authorization for Electronic Network Access* when logging on to the Internet, or sign the District's *Authorization for Electronic Network Access* form as a condition for using the District's electronic networks. The acceptance of terms stated in the pop up or signature on the *Authorization for Electronic Network Access* form provides consent for the District to monitor a user's electronic network use.

All users of the District's computers and electronic networks that 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 on the network.

The failure of any user to follow the terms of the *Acceptable Use of Electronic Networks* procedure, 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.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (l).
Enhances Education Through Technology, 20 U.S.C. §6751 et seq.
720 ILCS 135/0.01.
CROSS REF.: 5.100, 5.170, 6.40, 6.210, 6.230, 6.235, 6.260, 7.310
ADMIN. PROC.: 5.165-AP1, 5.165-AP2, 5.165-E1, 5.165-E2

Adopted: January 26, 2011
Reviewed:
Amended: