

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 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 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 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 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. 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 *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.

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 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), 6:220 (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 Behavior), 7:310 (Restrictions on Publications; Elementary Schools)

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 by Board Action 09/01/1998
 Amended by Board Action 11/14/2007
 Amended by Board Action 08/09/2012
 Board Review 08/08/2019
 Approved by Board Action 09/12/2019

Instruction

Administrative Procedure - Acceptable Use of the District's Electronic Networks

All use of the District's electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or legal action.**

Terms and Conditions

Acceptable Use - Access to the District's electronic networks must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - Use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator or Building Principal will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

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

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

Network Etiquette - The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- a. Be polite. Do not become abusive in messages to others.
- b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
- d. Recognize that email is not private. People who operate the system have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities.
- e. Do not use the networks in any way that would disrupt its use by other users.

- f. Consider all communications and information accessible via the networks to be private property.

No Warranties - The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of these procedures.

Security - Network security is a high priority. If the user can identify a security problem on the Network, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to the Network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the networks.

Vandalism - Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the web or on District websites or file servers without explicit written permission.

- a. For each re-publication (on a website or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the web address of the original source.
- b. Students and staff engaged in producing web pages must provide library media specialists with email or hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the website displaying the material may not be considered a source of permission.
- d. The *fair use* rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of Email - The District's email system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides email to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

- a. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an email account is strictly prohibited.

- b. Each person should use the same degree of care in drafting an email message as would be put into a written memorandum or document. Nothing should be transmitted in an email message that would be inappropriate in a letter or memorandum.
- c. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet *domain*. This domain is a registered name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the content of any and all email messages transmitted to external recipients.
- d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- e. Use of the School District's email system constitutes consent to these regulations.

Internet Safety

Internet access is limited to only those *acceptable uses* as detailed in these procedures. Internet safety is almost assured if users will not engage in *unacceptable uses*, as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the *Terms and Conditions* for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry 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 system administrator and Building Principals shall monitor student Internet access.

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 Act of 2001, 20 U.S.C §6751 et seq.
Harassing and Obscene Communications Act, 720 ILCS 135/0.01.

Superintendent Review September, 2009
Superintendent Review July, 2019

Instruction

Exhibit - Staff Authorization for Access to the District's Electronic Networks

This form accompanies Administrative Procedure 6:235-AP1, Acceptable Use of the District's Electronic Networks. Each staff member must sign this Authorization as a condition for using the District's Electronic Networks. Please submit this form to the Building Principal.

All use of the Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. Administrative Procedure 6:235-AP1, *Acceptable Use of the District's Electronic Networks*, does not attempt to state all required or prohibited behavior by users. However, some specific examples are provided. **The failure of any user to follow the terms of *Acceptable Use of the District's Electronic Networks*, will result in the loss of privileges, disciplinary action, and/or legal action.** The signature at the end of this document is legally binding and indicates that the individual has read the terms and conditions carefully and understands their significance.

Staff members need only sign this *Authorization for Access to the District's Electronic Networks* once while employed by the School District.

I understand and will abide by the *Acceptable Use of the District's Electronic Networks*. I understand that the District and/or its agents may access and monitor my use of the District's electronic networks, including the Internet, my email and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and disciplinary action and/or legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its School Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the District's electronic networks, including the Internet.

User Name *(please print)*

User Signature

Date

Superintendent Review, July 2019