INSTRUCTION

Administrative Procedure - Acceptable Use Electronic Network

All use of the Internet 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 proscribed 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 educational objectives of the District, or (b) for legitimate business use.

Privileges – The 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 a recommendation to the Superintendent regarding whether or not a user has violated theses procedures and may deny, revoke, or suspend access at any time; the Superintendent's decision is final.

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

a. 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;

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 network 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, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature;

h. Using another user's account or password;

i. Posting material authorized or created by another without his/her consent;

j. Posting anonymous messages or masquerading as someone else.

k. Using the network for commercial or private advertising;

l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate or misleading, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

m. Using the network 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 e-mail is not private. People who operate the system have access to all e-mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in any way that would disrupt its use by other users.

f. Consider all communications and information accessible via the network 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 relation 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 Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep the user's account and password confidential. Do

not use another individual's account without written permission from that individual. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

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.

Personal Use - Personnel may not use the Internet for personal use during their scheduled workday or contracted times. Employees may be asked to limit excessive use or discontinue personal use if the privilege is abused.

Personal Equipment Use on the Network- Staff can use personal electronic equipment on the district's network using a wireless connection only. Personal equipment must have current antivirus protection and be used predominately for work related activities. Before access is given to staff, they must sign 6:235-E1 and have it signed by their building administrator and technology staff. The signed forms will be kept in the district office.

Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.

a. For each re-publication (on a Web site 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 e-mail 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 Web site 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 graphic and text.

e. Student work may only be published if there is written permission from both the parent/guardian and student.

Use of E-Mail - the District's e-mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid 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 e-mail account is strictly prohibited.

b. Each person should use should use the same degree of care in drafting an e-mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail 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 this School District. Users will be held personally responsible for the content of any and all e-mail 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 e-mail 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, P.L. 106-554
Enhances Education Through Technology Act of 2001, 20 U.S.C. 6751 et seq.
Harassing and Obscene Communications Act, 720ILCS 135/0.01

ADOPTED: April 16, 1996
REVISED: October 5, 1999
REVISED : October 2, 2001
REVISED: October 9, 2009
REVISED March 17, 2011, September 9, 2011
REVIEWED: November 25, 2013