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 appropriate legal action.

Terms and Conditions

1. Acceptable Use - Access to the District's electronic network**s** 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.

2. 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 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.

3. Unacceptable Use - The user is responsible for his or her actions and activities involving the network***s***. Some examples of unacceptable uses are, but not limited to:

   a. Using the network***s*** 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 devirused including illegal peer-to-peer file sharing programs such as Kazaa, Frostwire, Limewire, eDonkey, etc…;

   c. Downloading 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 and network bandwidth;

   f. Hacking or gaining unauthorized access to resources or entities and using proxy sites or any other means to gain access to prohibited sites and areas on the network;

   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 network***s*** 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 network***s*** while access privileges are suspended or revoked.

INSTRUCTION

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

n. Accessing social networking sites that are not used for educational purposes such as MySpace, Facebook, Xanga, etc…;

o. Do not become abusive in messages to others.

p. Do not swear, or use vulgarities or any other inappropriate language.

q. Do not reveal personal information, including the personal addresses or telephone numbers of students or colleagues.

r. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

s. Do not use the network in any way that would disrupt its use by others.

t. User shall not use the network for any illegal activity including, but not limited to, unauthorized access including hacking.

u. Do not connect to a network unassociated with the district (with the exception of a cell phone).

4. 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.

5. 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.

6. 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 network*s*.

7. 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.

8. 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.

9. Copyright Web Publishing rules - Copyright law and District policy prohibit the re-publishing 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.

INSTRUCTION

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

b. 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.

c. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

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

10. Use of Electronic Mail, Text Messaging, and Social Media

a. The District's electronic 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 students and staff members in fulfilling their duties and responsibilities, and as an education tool.

b. 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 electronic mail account is strictly prohibited.

c. Each person will use the same degree of care in drafting an electronic 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.

d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain 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 electronic mail messages transmitted to external recipients.

e. 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.

f. Use of the School District's electronic mail system constitutes consent to these regulations.

11. User's Responsibility

a. Users may not share their account with anyone or leave the account open or unattended. Passwords are confidential. All passwords should be protected by the user and not shared or displayed.

b. Users are responsible for immediately notifying the Technology Department if any possible security problems or of damage to the computer to which they are assigned.

12. Use of Computer Hardware and Software

a. Only authorized individuals will install, service and/or maintain District-owned computer hardware.

b. No hardware, including cables or peripherals, may be moved from building to building, moved from the District, or loaned to another District employee without authorization from the Technology Department.

INSTRUCTION

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

c. Only software (on disk or downloaded) that is legally owned and/or authorized by the District may be installed on District computers.

d. The Technology Department's agents and/or Building Administrators have the right to remove any software from District owned equipment where the user cannot provide original copies of the software and/or appropriate license for the software.

13. Personal Technology

Definition: Personal technology is defined as any device that is not owned or leased by the District or otherwise authorized for District use and (1) transmits sounds images, text messages videos, or electronic information; (2) electronically records, plays, or stores information; (3) accesses the Internet or private communications or information networks. This includes, but is not limited to smartphones, tablets, etc.

a. For all personal technology unassociated with the District provided network [including but not limited to any network technologies, i.e. 3G, 4G] the Board expressly claims no responsibility for imposing content filters, blocking lists, or monitoring of its students' or employees' personal technology.

b. Where personal technology has been approved for use during school or school-sponsored activities the student or employee will assume all risks associated with the use of personal technology and adhere to the standards set forth for appropriate behavior as stated and signed in the Acceptable Use Policy at all times, regardless if one is connected to the District network or to another unassociated network.

c. For employees of the District, use of personal technology and social media for personal purposes is permitted within the District only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.

d. The district assumes no responsibility for a personal technology device that is lost, stolen, or damaged in any way.

e. The district will not expend any personnel or instructional time to support personal technology devices.

Internet Safety

1. Internet access is limited to only those "acceptable uses" as detailed in District policy and 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.

2. 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 in these procedures.

3. 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.

4. The system administrator and Building Principals shall monitor student Internet access.

INSTRUCTION

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

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777
Children's Internet Protection Act, (h) and (l).
Enhances Education Through Technology, 20 U.S.C. §6751, et seq.
Harassing and Obscene Communications Act, 720 ILCS 135/0.01

Adopted 9-16-97
Revised 12-14-98
Revised 6-18-01
Revised 12-17-01
Revised 03-19-07
Revised 11-19-07
Revised 06-18-12
Revised 11-18-13
Revised 10-17-16