Instruction

Administrative Procedure - Acceptable Use of the Electronic Networks

All use of the 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 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 appropriate legal action.**

Terms and Conditions

1. **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.

2. **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 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. 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 State or federal law;

    b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;

    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;

    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 network 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.

m. Using the network while access privileges are suspended or revoked.

n. Use of network for, or in support of any obscene or pornographic purposes including, but not limited to, the retrieving or viewing of any sexually explicit material. If a student authorized user inadvertently accesses such information, he or she must immediately disclose the inadvertent access to a teacher or an administrator. Other authorized users should report incidences to the network administrator. This will protect the user against allegations of intentionally violating this policy.

o. Use of the network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or "stalk" (cyberstalking) another individual.

p. Violation of any provision of the Illinois School Student Records Act (105 ILCS 10/1et seq.), which governs students' rights to privacy and the confidential maintenance of certain information including, but not limited to a student's grades and test scores.

q. Any form of unauthorized access, as stated above or otherwise.

4. **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 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.

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.

5. **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.

6. **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.

7. **Security** - All student authorized users are to report promptly any violations of this policy to their teacher or school principal. Teacher or school principal will report such violations to the Information Technology Manager or designee of the Superintendent in order to ensure network security.

In order to maintain the security of the system, authorized users are prohibited from engaging in the following actions:

a. Use of any unauthorized personal equipment attached, connected, and/or installed to district network.

b. Intentionally disrupting the use of the network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, spreading computer viruses, engaging in "hacking" of any kind, use of proxy or filter avoidance software or devices, and/or engaging in computer tampering of any kind.

c. Disclosing the contents or existence of computer files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients. Authorized users must not share logins or password(s) and unauthorized information regarding other users' passwords or security systems.

d. Network security is a high priority. If you can identify a security problem on the network, you must notify a system administrator. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. 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 or having a history of problems with other computer systems may be denied

access to the network.

8. **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.

9. **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 of line costs.

10. **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 republication (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 graphics and text.

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

11. **Use of Electronic Mail**

    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.

    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 electronic mail account

is strictly prohibited.

b. Each person should 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.

c. 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.

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 electronic mail system constitutes consent to these regulations.

12. **Online Activities**

a. Educational Purposes

Authorized users may create webpages as a part of a class activity. Material presented on a class website must meet the educational objectives of the class activity. The District has the right to exercise control over the content and/or style of the student webpages.

Only those students whose parent(s) or guardian(s) have completed the *Authorization for Electronic Network Access Form* Permission for Publication section may post their work or picture on student or school websites. Students whose work, likeness (as captured by photograph, video or other media) or voices are presented on a student website shall be identified by first name only for confidentiality and safety purposes.

b. Electronic Social Networking

While home-based web sites, message boards, blogs, forums, and other uses of home-based computers may be regarded as a benefit to a student's computer literacy, the student needs to be aware of the following:

Using a non-district computer, either during or outside of the regular school day,

such that the use results in material and/or substantial disruption to the school will constitute grounds to investigate whether the use violates applicable law (see Greenfield BOE vs Boucher, 1998) or district rules. Should such misuse be found, the school will implement appropriate consequences as defined in the acceptable use policy and the student discipline code. As district network use is a privilege, such violations may result in suspension of use of district network or other technology for a period of time based upon the seriousness of the offense's impact or a threat's ability to have caused material and/or substantial disruption were it carried out.

13. **Monitoring**

The District network is routinely monitored to maintain the efficiency of the system. Authorized users should be aware that use of network resources, including their use of e-mail, is subject to monitoring by the superintendent, technology director, or his/her designee. Any activities related to or in support of violations of this policy and/or the Student Handbook may be reported and will subject the user to sanctions specified either in the Student Handbook or in this policy. The district reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the user.

14. **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 is filtered in a manner to block 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.

15. **Definitions**

A. **Electronic Network Related Technologies and Access ("Network")** is the system of computers, peripherals, terminals, servers, databases, routers, hubs, switches and distance learning equipment connected to the District network. These components may function in conjunction with established hardwire or wireless LAN running over outside lines, including, but not limited to T -1, BRI, PRI, VPN, Dialup, Distance Learning Equipment, owned or leased by Harlem Schools.

B. **Cyberstalking** is knowingly harassing another person or persons through the use of electronic communication.

C. **Damage** means any impairment to the integrity or availability of data, a program, a system, or information.

D. **Distance Learning Equipment** is a means for providing meetings, educational or professional courseware and workshops utilizing video and/or audio conferencing equipment, and/or media management systems to distribute video to individual classrooms and offices in schools.

E. **Electronic Mail (e-mail)** consists of all electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments.

F. **Electronic Social Networking** includes the use of any electronic form of communication including but not limited to chat rooms, email, forums, article forwarding, instant messaging, text messaging, blogs, message boards, document forwarding from home, libraries, or other outside sources and other uses of electronic communication for non-educational purposes.

G. **Hacking** is any illegal or unlawful entry into an electronic system to gain secret unauthorized information.

H. **Harass** means to engage in a knowing and willful course of conduct directed at a specific person or persons that alarms, torments, or terrorizes that person or persons.

I. **Loss** means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

J. **Internet** a collection of worldwide networks and organizations that contain millions of pages of information.

K. **Other Electronic Devices** include, but are not limited to, cellular telecommunication devices such as cellular phones, pagers, text communication pagers, two-way text pagers, and personal digital assistants that may or may not be physically connected to the network infrastructure.

L. **Password** is a secret word or series of letters, numbers and/or other characters that must be used to gain access to a network, a service or the Internet, and/or to

modify certain software (such as parental controls).

M. **Sexually explicit material** means any material displaying sexual content that does not directly correspond to approved curriculum.

N. **Authorized User** is anyone who has signed the current network acceptable use policy and has had it accepted by the District Superintendent or his/her designee.

O. **Unauthorized access** entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and/or changing computer resources without authorization.

P. **Website** is a page and/or a collection of "pages" or files on a network that are linked together

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.

APPROVED: May 31, 2011