

## 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

The term *electronic networks* includes all of the District's technology resources, including, but not limited to:

1. The District's local-area and wide-area networks, including wireless networks (Wi-Fi), District-provided Wi-Fi hotspots, and any District servers or other networking infrastructure;
2. Access to the Internet or other online resources via the District's networking infrastructure or to any District-issued online account from any computer or device, regardless of location;
3. District-owned and District-issued computers, laptops, tablets, phones, or similar devices.

**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 may result in a cancellation of those privileges, disciplinary action, and/or appropriate legal action. 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 electronic networks. Some examples of unacceptable uses are:

- a. Using the electronic networks for any illegal activity, including violation of copyright or other intellectual property rights or contracts, or transmitting any material in violation of any State or federal law;
- b. Using the electronic networks to engage in conduct prohibited by board policy;
- c. Unauthorized downloading of software or other files, regardless of whether it is copyrighted or scanned for malware;
- d. Unauthorized use of personal removable media devices (such as flash or thumb drives);
- e. Downloading of copyrighted material for other than personal use;
- f. Using the electronic networks for private financial or commercial gain;
- g. Wastefully using resources, such as file space;
- h. Hacking or attempting to hack or gain unauthorized access to files, accounts, resources, or entities by any means;
- i. Invading the privacy of individuals, including the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature, such as a photograph or video;
- j. Using another user's account or password;
- k. Disclosing any network or account password (including your own) to any other person, unless requested by the system administrator;

- l. Posting or sending material authored or created by another without his/her consent;
- m. Posting or sending anonymous messages;
- n. Creating or forwarding chain letters, spam, or other unsolicited messages;
- o. Using the electronic networks for commercial or private advertising;
- p. Accessing, sending, posting, publishing, or displaying any abusive, obscene, profane, sexual, threatening, harassing, illegal, or knowingly false material;
- q. Misrepresenting the user's identity or the identity of others; and
- r. Using the electronic networks while access privileges are suspended or revoked.
- s. 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.
- t. 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.
- u. 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.

**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 the District's electronic networks are not private. People who operate District technology have access to all email and other data. Messages or other evidence 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 electronic 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** - By using the District's electronic networks, the user agrees to indemnify the 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 or suspects a security problem on the network, the user must promptly notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep user account(s) and password(s) 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.

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.

Non-District Device (NDD) includes any personally owned device, any device issued by external entities or any device not approved and distributed by the District IT Department.

NDD's may be connected to the Harlem School District's wireless network by a District staff member or Students 9-12 under the following guidelines/constraints:

a. All rules and regulations stated within Harlem's Acceptable Use Policy (AUP) still apply to NDD's.

b. Internet Access Only\

NDD's may only be used to access Internet resources. Access will not be given to internal network resources such as printers or files stored on internal servers. As such, additional care must be taken with regard to storage of personal and confidential (student/staff) information of any kind via the Internet (e.g. Dropbox, iCloud, Google Driver, Microsoft SkyDrive, etc.)

C. The Harlem School District applies web filtering policies to this network that are consistent with District staff member filtering on District owned devices. However, as NDD's are connected to a public network, the Harlem School District does not accept responsibility for any damage or loss. It is the sole responsibility of the user of the device to ensure that it is protected.

d. Device Support

The connection of the device(s) is/are allowed, but there will be no technical support of any NDD by the Harlem IT Department. Resources covering how to connect an NDD device to the wireless network will be made available online, but it will fall to the provider/vendor of the device to support the device.

**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 malware, such as viruses and spyware.

**Telephone Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, texting or data use 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 Internet or on District websites or file servers/cloud storage 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 District. The 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 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 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 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, such as spam or potential phishing emails, 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 District's email system constitutes consent to these regulations.

### 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.

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.

20 U.S.C. §7131, Elementary and Secondary Education Act.

47 U.S.C. §254(h) and (l), Children's Internet Protection Act.

720 ILCS 135/, Harassing and Obscene Communications Act.

APPROVED: December 13, 2021