

CHAPTER 7: INTERNET, TECHNOLOGY AND PUBLICATIONS

Internet Acceptable Use

PRESS 6:235 (MSH 7.10)

All use of electronic network use must be consistent with the school's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These rules 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 rules will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Acceptable Use - Access to the electronic network 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 - The use of the electronic network 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 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 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, 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; 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 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 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 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 Internet, 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 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.

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 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.

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 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 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.

Use of the School District's email system constitutes consent to these regulations.

Cell Phones: Cell phone usage at the JR/SR high school will be limited to the hallway between classes and during lunch in the cafeteria and only in silent mode. Cell phone usage at the elementary school is limited to before or after school, unless prior permission from the teacher. Cell phone use during class will result in confiscation and may be picked up in the office after school. Other electronic devices brought to school for educational purposes will be the sole responsibility of the owner.

Protection Act
(MSH 7.40)

School districts throughout the State of Illinois contract with different educational technology vendors for beneficial K-12 purposes such as providing personalized learning and innovative educational technologies, and increasing efficiency in school operations.

Under Illinois' Student Online Personal Protection Act, or SOPPA (105 ILCS 85/), educational technology vendors and other entities that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes are referred to in SOPPA as *operators*. SOPPA is intended to ensure that student data collected by operators is protected, and it requires those vendors, as well as school districts and the Illinois State Board of Education, to take a number of actions to protect online student data.

Depending upon the particular educational technology being used, our District may need to collect different types of student data, which is then shared with educational technology vendors through their online sites, services, and/or applications. Under SOPPA, educational technology vendors are prohibited from selling or renting a student's information or from engaging in targeted advertising using a student's information. Such vendors may only disclose student data for K-12 school purposes and other limited purposes permitted under the law.

In general terms, the types of student data that may be collected and shared include personally identifiable information (PII) about students or information that can be linked to PII about students, such as:

- Basic identifying information, including student or parent/guardian name and student or parent/guardian contact information, username/password and student ID number
- Demographic information
- Enrollment information
- Assessment data, grades, and transcripts
- Attendance and class schedule
- Academic/extracurricular activities
- Special indicators (e.g., disability information, English language learner, free/reduced meals or homeless/foster care status)
- Conduct/behavioral data
- Health information
- Food purchases
- Transportation information
- In-application performance data
- Student-generated work
- Online communications
- Application metadata and application use statistics
- Permanent and temporary school student record information

Operators may collect and use student data only for K-12 purposes, which are purposes that aid in the administration of school activities, such as:

- Instruction in the classroom or at home (including remote learning)
- Administrative activities
- Collaboration between students, school personnel, and/or parents/guardians
- Other activities that are for the use and benefit of the school district