Superintendent's Regulation 1950-R

STUDENT NETWORK ACCEPTABLE USE

Approved Upon Superintendent's Initials

8/13/14
Date

This Regulation provides information about the privileges and responsibilities of using the Internet and the Rochester City School District Network as part of our student's educational experience.

1. Responsibilities

   The Rochester City School District has taken reasonable precautions to restrict access to "harmful matter" and to materials that do not support approved educational objectives. "Harmful matter" refers to material that, taken as a whole by the average person applying contemporary statewide standards, describes in an offensive way material that lacks serious literary, artistic, political or scientific value for minors. The teachers and staff will choose resources on the Internet that are appropriate for classroom instruction and/ or research for the needs, maturity, and ability of their students. The Rochester City School District takes no responsibility for the accuracy or quality of information from Internet sources. Use of any information obtained through the Internet is at the user's risk.

2. Acceptable Use

   The purpose for schools having access to the District Network and the Internet is to enhance teaching and learning by providing access to 21st century tools and resources as well as online instruction. Use of another organization's data networks (e.g. Cell Phone Carriers) or computing resources must comply with rules of that network as well as District User policies.

3. Prohibited Uses

   a. Transmission of any material in violation of any federal or state law, and district policy is prohibited. This includes, but is not limited to, the distribution of:

      1. Any information used to intimidate or harass, or intended to harm, insult, or humiliate another in a deliberate, repeated, hostile or unwanted manner;
      2. Any defamatory, inappropriate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or illegal material;
      3. Advertisements, solicitations, commercial ventures or political lobbying;
      4. Any information that encourages the use of controlled substances or the use of the system for the purpose of inciting crime;
      5. Any material that violates copyright laws.

b. Any vandalism, unauthorized access, "hacking," or tampering with hardware or software, including introducing "viruses" or pirated software, is strictly prohibited.
c. The district reserves the right to monitor internet/intranet, e-mail, and networked application usage. No student or employee should have any expectation of privacy as to his/her usage. The district reserves the right to inspect any and all files on district computers or district servers connected to district networks and to take custody and possession of those files and computers.

Warning: The use of The District Network and the Internet is a privilege, not a right, and inappropriate use may result in the cancellation of Network privileges.

4. Network Rules and Etiquette

The use of The District Network and the Internet requires that students abide by district rules of network use and etiquette. These include, but are not limited to, the following:

a. Be polite. Do not send abusive messages to anyone.
b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Anything pertaining to illegal activities is strictly forbidden. Note: E- mail and web-based programs are not private and are subject to review by district staff. People who operate the system have access to all mail. Messages relating to, or in support of, illegal activities must be reported to appropriate authorities.
c. Maintain privacy. Do not reveal the personal address, phone numbers, personal web sites or images of yourself or other persons. Before publishing a student's picture, first name, or work on the Internet, the school must have on file a parent release authorizing publication.
d. Cyberbullying is considered harassment.
e. Respect copyrights. All communications and information accessible via the network are assumed to be the property of the author and should not be reused without his/her permission.
f. Do not disrupt the District Network.

5. Security

Security on any computer system is a high priority. If you feel you can identify a security problem on the District Network, notify the district Educational Technology Department or the Information Management & Technology Department either in person, in writing, or via the network. Do not demonstrate the problem to other users. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the District Network and the Internet.