Computer Network System Use

The Board of Education of the Newburgh Enlarged City School District is committed to the goal of improved student learning and effective teaching. The Board believes that access to computer networks, including the Internet and other technologies, can be an effective and valuable educational and research tool. The Board further believes that the computer network system, through software applications, online databases, bulletin boards and the Internet, and emerging features and uses of an electronic network, will significantly enhance student learning, as well as provide local, statewide, national and global communications opportunities for staff and students. Therefore, it is the policy of the Board to support and encourage the use of computers and computer-related technology in order to support open research and education in the District. The use of the computer network system for other purposes, including but not limited to for-profit or commercial activity, personal business or illegal activity is prohibited.

All users of the District's computer network system, including but not limited to electronic equipment, electronic mail and the Internet, must understand that use is a privilege, not a right, and that such use entails responsibility on the part of the user. Computer access will be provided by the District to all students and staff members in accordance with this Policy. In order to assure the integrity of the computer network system in the District, each account holder must agree to act responsibly and to comply with this Policy and its implementing Regulations. Any parent/guardian who does not want his/her child to have access to the District's computer network system must notify the District in writing. The Superintendent of Schools shall develop rules and regulations governing the use and security of the District's computer network system.

Teacher Web Pages

All web pages residing on a District-supported server or service are the property of the Newburgh Enlarged City School District. Commercial use, use for the pursuit of personal or financial gain, advertising, soliciting, as well as use for any personal purpose are prohibited. The Superintendent of Schools and/or his/her designee may suspend webpage access at any time if an individual fails to adhere to the protocol or requirements stated herein. Each teacher/staff is responsible for the content posted on his/her webpage hosted on the District-supported servers/services and will follow all District procedures. Teacher web pages may link only to sites that are of educational significance and sites relating to the curriculum and activities of the District.

Internet Safety

Internet access is provided with the understanding that the District cannot control the content available on the Internet. While the vast majority of sites available provide a wealth of useful information to staff and students, some sites may contain information that is inaccurate, offensive, defamatory or otherwise inappropriate for students. The District does not condone or permit the use of such materials in the school environment and makes good faith efforts to limit access by students to such inappropriate materials.

The Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and

- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Upon the approval of the Superintendent or his/her administrative designee, any such measures may be disabled or relaxed for staff members conducting bona fide investigations in accordance with criteria established by the Superintendent or his/her designee.

The Superintendent or his/her designee also shall develop and implement procedures that provide for the safety and security of students using direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access or other unlawful activities; and access to inappropriate matter on the Internet and World Wide Web.[1] The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The computer network coordinator shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's

[1] In accordance with the Children's Internet Protection Act,

- *Child pornography* refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- *Harmful to minors* means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

acceptable use policy. Failure to comply may result in disciplinary action including, but not limited to, the suspension or revocation of computer access privileges.

The district shall also provide age-appropriate instruction regarding appropriate online behavior, including:

1. interacting with other individuals on social networking sites and in chat rooms, and
2. cyberbullying awareness and response.

Instruction will be provided even if the district prohibits students from accessing social networking sites or chat rooms on district computers.

Privacy

Users acknowledge that the network administrator may periodically need to review on-line activities in the course of performing routine maintenance of the system. Users further acknowledge that if there is reasonable suspicion of a user having violated this Policy or its implementing regulations, or any applicable law, the network administrator and/or appropriate school official may require access to his/her files, including private correspondence and private files, to review on-line activities. Any administrator reviewing such files in accordance with this Policy shall not be subject to any claims arising out of such review.

The School District, however, prohibits the unauthorized disclosure, use and dissemination of personal information regarding minors by its officers, employees or agents.

Failure by any user to comply with District policy or regulations regarding the use of the computer network system may result in suspension and/or revocation of computer access and/or related privileges. Further, a breach in the terms of this Policy and Regulations may be considered an act of insubordination, which may result in disciplinary action in accordance with law, and applicable collectively negotiated agreements and legal action where appropriate.