

(X) Required

Local

Notice

INTERNET SAFETY

The Millbrook Central School District Board of Education is committed to undertaking efforts that serve to make safe for children the use of district information technology resources (including but not limited to computers and networks) for access to the Internet. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, 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.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district technology resources; 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 by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The information technology (IT) coordinator designated under the district's policy on the acceptable use of information technology resources in instruction (policy 4526) shall monitor and examine all district IT 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 network, including the Internet, 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 policy on the acceptable

MCSD 4000 Policy Series: Instruction

4526.1

use of information technology resources in instruction (policy 4526). Failure to comply may result in disciplinary action including, but not limited to, the revocation of technology resource access privileges.

As part of this policy, and the district's policy on acceptable use of information technology resources in instruction (policy 4526), 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 technology resources.

Cross-ref: 4526, Acceptable Use of Information Technology in Instruction
8260, Staff Use of Information Technology Resources and Data Management

Ref: Children's Internet Protection Act, Public Law No. 106-554
Broadband Data Services Improvement Act/ Protecting Children in the 21st Century Act, Public Law No. 110-385
18 USC §2256
47 USC §254
20 USC §6777

Adoption date: June 7, 2022

INTERNET SAFETY REGULATION

The following rules and regulations implement the Internet Safety Policy (4526.1) adopted by the Millbrook Central School District Board of Education to make safe for children the use of district computers for access to the Internet.

I. Definitions

In accordance with the Children’s Internet Protection Act,

- “Child pornography” refers to any visual depiction, including any photograph, film, video, picture or information technology resource generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (b) such visual depiction is a digital image, technology device image, or technology device-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or (c) such visual depiction has been created, adapted or modified to appear that an identifiable minor is 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.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district information technology resources to visual depictions on the Internet that are obscene, child pornography or harmful to minors.
- The district’s Information Technology Director shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The Information Technology Director or his or her designee may disable or relax the district’s Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

MCS D 4000 Policy Series: Instruction

4526.1-R

- The Information Technology Director shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's Information Technology Director shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's information technology (IT) network for accessing the Internet and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's network shall have no expectation of privacy regarding any such materials.
- Except as otherwise authorized under the district's Acceptable Use of Information Technology Resources in Instruction policy (4526), students may use the district's network to access the Internet only during supervised class time, study periods or at the school library, on campus before or after school, and exclusively for research related to their course work.
- Staff supervising students using district information technology resources shall help to monitor student online activities to ensure students access the Internet, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's Information Technology Director shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other information technology systems), and other unlawful activities.

IV. Training

- The district shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.

MCSD 4000 Policy Series: Instruction

4526.1-R

- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of information technology resource access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Adoption date: June 7, 2022