( ) Required
(X) Local
(X) Notice

ACCEPTABLE USE OF INFORMATION TECHNOLOGY IN INSTRUCTION

The Millbrook Central School District Board of Education is committed to optimizing student learning and teaching. The Board considers student access to information technology (including but not limited to computers, network, and the Internet), to be a powerful and valuable educational and research tool, and encourages the use of information technology in district classrooms solely for the purpose of advancing and promoting learning and teaching.

The network can provide a forum for learning various software applications and through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communication opportunities for staff and students.

The availability of information through electronic sources has significantly altered the landscape for schools by opening classrooms to a broader array of resources. In the past, instructional and library materials could usually be screened prior to use, by educators intent on subjecting all such materials to reasonable selection criteria. Board Policy requires that all such materials be consistent with district-adopted guides, supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of the students. Electronic information which is publicly available from any file server in the world, will open classrooms to information sources which have not been screened by educators for use by students of various ages. As a result, research skills are now fundamental to preparation of our students to be good citizens and future employees. The Board expects that staff will provide guidance and instruction to students in the appropriate evaluation and use of electronic resources.

All users of the district's information technology resources and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. Students are responsible for good behavior on school networks just as they are in a classroom or school hallway. The network is provided for students to conduct research, complete assignments, and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

The Superintendent of Schools shall establish regulations governing the use and security of the district's network. All users of the district's information technology resources shall comply with these policies and regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of access privileges.

Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. No user may disclose, use, or disseminate personal identification information regarding minors without authorization. Students encountering information or messages they deem dangerous or inappropriate on the web or when using electronic mail or direct communications tools should immediately notify their teacher or other adult staff.

The district's Director of Technology has been designated by the Superintendent as responsible for the information technology (IT) network and oversight of the use of district IT resources. The Director of Technology will prepare in-service programs for the training and development of district staff in IT skills, and for the incorporation of IT in appropriate subject areas.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Director of Technology. The Director of Technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

The Superintendent, working in conjunction with the designated purchasing agent for the district, the Director of Technology and the instructional materials planning team, will be responsible for the purchase and distribution of IT software and hardware throughout district schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

Cross-ref: 4526.1, Internet Safety
5300, Code of Conduct
5695, Student Use of Personal Electronic Devices
8260, Staff Use of Information Technology Resources and Data Management

Adoption date: June 7, 2022

ACCEPTABLE USE OF INFORMATION TECHNOLOGY IN INSTRUCTION REGULATION

The following rules and regulations govern the use of the district's information technology (IT) network system and access to the Internet.

I. Administration

- The Director of Technology will oversee the district's network.
- The Director of Technology shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Director of Technology shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The Director of Technology shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations governing use of the district's network.
- The Director of Technology shall take reasonable steps to protect the network from viruses or other software that would compromise the network.
- All student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the building where the student is enrolled.

II. Internet Access

- Students will be provided Internet access during class time, during the school day when students are not in class, and on campus before or after school hours.
- Students will be provided with individual accounts to access the network and Internet.
- Students may have Internet access after submitting a Student User Agreement form signed by the student and their parent/guardian for educational purposes.
- Students may have access to school provided e-mail, based upon school policy or Principal recommendation, after submitting a Student User Agreement form signed by the students and their parent/guardian.
- Student Internet access may be restricted depending on the grade level.
- In order to access the Internet students must use the district's network.
- All users will be prohibited from: accessing social networking sites; playing online games; purchasing or selling anything online (unless authorized for district purposes); personal email services; and watching videos online (unless authorized for a school purpose).
- Students may not participate in chat rooms, instant messaging, or other forms of direct communication without explicit permission from a teacher or adult staff member unless for educational purposes.
- Students may construct web pages using district IT resources within the context of instruction related assignments or supervised school activities.

- All web content published by students and student organizations on the district's network will be subject to treatment as district sponsored publications. Accordingly, the district reserves the right to exercise editorial control over such publications.
- Students will not be assigned email accounts for personal use, nor may students access their personal (home use) email accounts while on campus or when using district owned equipment. However, in the context of particular coursework and/or to further education and/or job placement and based on school policy, students may be assigned a district email account to be used within a password protected, limited access environment as per Administration. No email account will be shared by multiple students.
- A staff member will provide general supervision to promote appropriate student Internet use during class sessions; however students shall always be expected to comply with appropriate use requirements when accessing the Internet in the school setting.

III. Acceptable Use and Conduct

- Access to the district's IT is provided solely for educational purposes and research consistent with the district's mission and goals.
- Use of the district's IT is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Use of a generic or anonymous login (e.g., guest, student, or teacher) is prohibited without the written consent of a district administrator. In order to promote individual user security, users should change their passwords periodically.
- Only those network users with written permission from a district administrator who have properly registered their device with the district, or who have been issued a district-owned device, may access the district's system from off-site (e.g., from home).
- All network/email users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are all inappropriate.
- Network/email users identifying a security problem on the district's network must immediately notify the appropriate teacher, administrator or Director of Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified.
- Any network/email user identified as a security risk or having a history of violations of district acceptable use of information technology guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activities concerning use of the district's IT resources. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district IT network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using another user's account or password.
- Using the network to send anonymous messages or files.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network/email to receive, transmit or make available to others a message that is inconsistent with the district's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages not related to education, educational programs, or employment.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal storage devices or media on the district IT equipment and/or network without the permission of the appropriate district official or employee.
- Using district IT resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any information, IT resources, or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while access privileges are suspended or revoked.

- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

V. No Privacy Guarantee

Students using the district's network should not expect, nor does the district guarantee privacy for any use of the district's network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's network.

VI. Sanctions

All users of the district's IT resources are required to comply with the district's policy and regulations governing the district's network. Failure to comply with the policy or regulation may result in disciplinary action consistent with the Student Code of Conduct, as well as suspension and/or revocation of access privileges. In an appropriate case, law enforcement and other authorities will be contacted.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material, or material protected by trade secret. Users must respect all intellectual and property rights and laws.

Any student user who is suspected of using the district network or Internet in a manner that would violate this policy or any other District policy, rule and/or regulation, or would violate any State or Federal law or regulation, will be notified of the alleged violation and provided with an opportunity to respond to and discuss the allegation.

VII. District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or any other errors or omissions. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's network or the Internet.

Further, even though the district may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: June 7, 2022