8630

STAFF USE OF INFORMATION TECHNOLOGY RESOURCES AND DATA MANAGEMENT

The Millbrook Central School District (MCSD) Board of Education recognizes that information technology (including but not limited to computers, network, and the Internet) is a powerful and valuable educational and research tool and, as such, is an important part of the instructional program. In addition, the district depends upon information technology as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Boards expectations in regard to these different aspects of the district's information technology (IT) resources.

General Provisions

The Superintendent shall be responsible for designating a IT coordinator who will oversee the use of district IT resources. The IT network coordinator will prepare in-service programs for the training and development of district staff in IT skills, appropriate use of IT and for the incorporation of IT in subject areas.

The Superintendent, working in conjunction with the designated purchasing agent for the district, the IT network coordinator, and the Assistant Superintendent for Curriculum & Instruction, will be responsible for the purchase and distribution of IT resources throughout the schools. They shall prepare and submit for the Board's approval a comprehensive multi-year IT plan which shall be revised as necessary to reflect changing technology and/or district needs.

The Superintendent, working with the IT coordinator, shall establish regulations governing the use and security of the district's IT resources. The security and integrity of the district network and data is a serious concern to the Board and the district will make every reasonable effort to maintain the security of the system. All users of the district's IT resources shall comply with this policy and regulation, as well as the district's Acceptable Use of Information Technology in Instruction and Internet Safety policies (4526 & 4526.1). Failure to comply may result in disciplinary action, as well as suspension and/or revocation of access privileges.

All users of the district's IT resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the district's IT resources must not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of district technology. The district reserves the right to access and view any material stored on district IT equipment or any material used in conjunction with the district's IT resources.

Management of Electronic Records

The Board recognizes that since district data is managed by information technology, it is critical to exercise appropriate control over electronic records, including financial, personnel and student information. The Superintendent, working with the IT coordinator and the district's business official, shall establish procedures governing management of electronic/digital records. The procedures will address:

- Passwords (log-in credentials?),
- system administration,
- separation of duties,
- remote access,
- data back-up (including archiving of e-mail),
- records retention, and
- disaster recovery plans.

This policy is subject to change. Access to district information technology shall terminate upon student graduation or withdrawal from the district or staff member suspension from or termination of employment. The district reserves the right to restrict or terminate information network access at any time for any reason. The district further reserves the right to monitor network activity as it sees fit in order to maintain the integrity of the network and to monitor responsible use. School and districtwide administrators will make the final determination as to what constitutes unacceptable use.

Review and Dissemination

Since information technology is a rapidly changing areas, it is important that this policy be reviewed periodically by the Board and the district's internal and external auditors. The regulation governing appropriate IT use will be distributed annually to staff and students and will be included in both employee and student handbooks.

Cross-ref: 1120, School District Records
4526, Acceptable Use of Information Technology in Instruction
4526.1, Internet Safety
6600, Fiscal Accounting and Reporting
6700, Purchasing
8635, Information Security Breach and Notification

Adoption date: June 21, 2010
Revision date: September 4, 2012

STAFF USE OF INFORMATION TECHNOLOGY RESOURCES AND DATA MANAGEMENT REGULATION

The following rules and regulations govern the use of the district's information technology, including but not limited to the computer or information systems network, employee access to the Internet, and management of electronic records (hereinafter “network”).

I. Administration

- The Superintendent of Schools shall designate an IT coordinator to oversee the district's network.
- The IT coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The IT coordinator shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery plan and will comply with the requirements for records retention in compliance with the district’s policy on School District Records (1120).
- The IT coordinator 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 IT coordinator 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 (including policy 4526, Instructional Use of Information Technology Resources, and policy 4526.1, Internet Safety) governing use of the district's network.
- The IT coordinator 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 attends. All employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district technology office.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the IT coordinator, will ensure the proper segregation of duties in assigning responsibilities for IT resources and data management.

II. Internet Access

District employees and third party users are governed by the following regulations:

- Employees will be issued a district e-mail account.
- Employees are expected to review their e-mail daily, unless precluded from doing so by other scheduled responsibilities or in the event of their absence from work.

- The district will archive all e-mail records according to procedures developed by the IT coordinator.
- Employees may access the Internet for education-related and/or work-related activities only.
- Employees shall refrain from using IT resources for personal use, commercial purposes or for soliciation.
- **Employee use of personally owned devices is permitted only when the device has been properly registered with the district. Only the person who registered the device is permitted to use the device for connecting to the Internet. The device should not be used by any other person unless they are under direct supervision by the registered user. The district is not responsible for the maintenance, repair or replacement of any personally owned devices. Internet use for curricular and/or school district communication activities on personally owned devices must be via the district's filtered Internet portal.**
- All web content published by faculty or staff on the district's network will be subject to treatment as district sponsored publications. Accordingly, the MCSD reserves the right to exercise editorial control over such publications.
- Employees are advised that they must not have an expectation of privacy in the use of the district's IT resources.
- Use of IT resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to **all staff and third party users** of the district's IT resources:

- Access is provided solely for educational and/or research purposes and management of district operations consistent with the district's mission and goals.
- Use is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- All network users will be issued a login name and password. In order to promote individual user security, users should change their passwords periodically**, or whenever it is suspected that their password is no longer secure**. The user should also report this to the IT coordinator.
- Each individual in whose name an access account is issued is responsible at all times for its proper use. **No staff member will provide any third party with their username and/or passwords, nor expose the same to public view. While signed into the network, a staff member may not leave any workstation unattended and in an unsecured state at any time. Users may be held responsible for problems arising from the use of their accounts.**
- Only those users with written permission from a district administrator may access the district's secured servers from off-site (e.g., from home).
- **Staff members with access to student records and information may not use, share, or release such records and information except as authorized by the District and/or State and Federal law.**

- All users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Users identifying a security problem related to the district's IT resources must immediately notify appropriate staff.
- Any user identified as a security risk or having a history of violations of district use guidelines may be denied access.

IV. File/Media Access, Licensing and Copyright

The following regulations apply to all staff and third party users of the district's IT resources:

- **Staff members must adhere to all copyright laws related to software, print, data, video, and attributions of authoring. The unauthorized copying, transfer, installation, or printing of licensed or copyrighted materials is prohibited.**
- **The creation, distribution, transmission, access, or use of any material in violation of Federal or State Law is prohibited.**
- **The creation, distribution, transmission, access, or use of threatening, obscene, harassing, lewd, confidential, discriminatory, or offensive materials is prohibited.**
- **The use of streaming audio, video, or other Web and network media is limited to educational use only.**
- **Staff members shall not vandalize, read, modify, edit, delete or otherwise engage in unauthorized use of another user's files.**

V. Prohibited Activity and Uses

The following is a list of prohibited activity for **all staff and third party users** concerning use of the district's network. Any violation of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Use for commercial activity, including advertising, solicitation of funds, political advertising, campaigning or lobbying, or for personal gain.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district network.
- Use to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Use to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- **Cyberbullying, hate mail, defamation, harassment of any kind, or discriminatory jokes or remarks**
- **Posting, sending, or storing information that endangers, threatens, or intimidates others**

- Use of another's account, username or password.
- Use to send anonymous messages or files.
- **Attempting to bypass/circumvent content filters**
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- 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.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Use for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal storage devices on the district's IT resources without the permission of the appropriate district administrator.
- **Use of "hacking tools", installation of viruses**
- **Installing or using keylogger programs on district IT resources**
- Using district IT resources for fraudulent purposes or financial gain.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer 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.
- Use while your access privileges are suspended or revoked.
- **Invading the privacy of individuals or entities (e.g. using someone else's name or account) or misrepresenting other users on the network**
- Use in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.

VI. Staff Supervision of Students

- **A responsible staff member will provide appropriate supervision to students using computer resources during all scheduled class times. Staff members should be familiar with all applicable Student Policies in effect, and will ensure that students receive appropriate instruction related to the student policies prior to students' use of computer resources during class times for assigned work.**
- **MCSD faculty and staff must ensure that students are using technology responsibly in the educational setting at all times. As such, no students will be permitted to use technology in MCSD unless under the direct supervision of a faculty or staff member.**
- **Any device approved by a faculty member to be used in the classroom or library on a regular basis to support student learning (laptop, iPad, Kindle) must also be approved by school administration and registered prior to use. An electronic device that also**

serves as a personal phone is NOT considered a device that can be used in the classroom on a regular basis and WILL NOT be approved for registration.

- **The use of unregistered personal student devices during school hours will only be permitted when students are explicitly told they may use such a device by a faculty member in the course of their instruction in his/her particular classroom.**
- **Faculty/staff are not permitted to share registration codes with students. Faculty/staff are not permitted to allow students to use his/her personal devices.**
- **It is the responsibility of the supervising faculty/staff member to immediately report all misuse, vandalism and other student policy violations to the appropriate administrator.**
- **Only students who have submitted an Internet Use permission form signed by both themselves and his/her parent/guardian are permitted to use District computer resources with adult supervision.**

VII. No Privacy Guarantee

Users of the district's IT should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any other use of the district's IT resources. 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 IT infrastructure.

VIII. Sanctions

All users of the district's IT resources are required to comply with the district's policy and regulations governing them. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of access privileges.

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 staff user who is suspected of using the 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 in a manner consistent with law and applicable collective bargaining agreement.

IX. 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.

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 computer 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 21, 2010
Revision date: September 4, 2012