MILLTOWN BOARD OF EDUCATION
Milltown, New Jersey

Policy

FILE CODE: 6142.10
_____ Monitored
_X_ Mandated
_X_ Other Reasons

INTERNET SAFETY AND TECHNOLOGY

The Milltown Board of Education shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, statewide, national and global communications opportunities for staff and students. Educational technology shall be infused into the district curriculum to maximize student achievement of the Core Curriculum Content Standards.

It is the policy of the district to establish safe and effective methods for student and staff users of the district's technological resources and to:

A. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

B. Prevent unauthorized access and other unlawful online activity;

C. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

D. Comply with the Children's Internet Protection Act (CIPA).

COMPLIANCE WITH CIPA

Filters Blocking Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the school district online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

A. Unauthorized access, including so-called "hacking," and other unlawful activities; and

B. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the school district staff to educate, supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the chief school administrator or his or her designee.

INTERNET SAFETY TECHNOLOGY (continued)

The chief school administrator or his or her designee shall ensure that students and staff who use the school internet facilities receive appropriate training including the following:

A. The district established standards for the acceptable use of the internet;

B. Internet safety rules;

C. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;

D. Cyberbullying (board policy 5131.1 Harassment, Intimidation and Bullying) awareness and response.

Student use of the Internet shall be supervised by qualified staff.

Policy Development

The district Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

ACCEPTABLE USE OF THE INTERNET

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district's system of electronic communication shall include access to the Internet for students and staff.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The Milltown Board of Education cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access to and use of the Internet.

The board designates the chief school administrator as the coordinator of the district system. He/she shall recommend to the Milltown Board of Education qualified staff persons to ensure provision of individual and class accounts necessary for access to the Internet, designation of quotas for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system.

Each principal shall coordinate the district system in his/her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that students are adequately supervised when using the system; maintaining executed user agreements; and interpreting this acceptable use policy at the building level.

INTERNET SAFETY TECHNOLOGY (continued)

Access to the System

This acceptable use policy shall govern all use of the system. Sanctions for student misuse of the system shall be included in the disciplinary code for students, as set out in regulations for policy 5131 Conduct/Discipline. Employee misuse may result in appropriate discipline in accord with the collective bargaining agreement and applicable laws and regulations.

The board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

Guest Network Access

Access to the school district's filtered wireless network utilizing school issued or personal wireless devices shall be made available to visitors who are approved professional development providers or other educational professionals as approved by Superintendent. Visitors shall acknowledge and agree to the district guest network disclaimer and assurances (board policy 6142.10).

Conditions of use for the district's network shall be permitted as long as the user's actions:

A. Comply with the responsibilities specified in the District's Acceptable Use Policy (AUP) for Technology);

B. Impose no tangible costs to the district;

C. Do not unduly burden the district's computers, or network resources;

D. Have no adverse effect on an employee's job performance or on a student's academic performance;

E. Do not cause a substantial disruption to the educational environment.

The district IT coordinator shall ensure that network access areas issued to guests comply with all board policies regarding the privacy and confidentiality of students and staff. The IT coordinator shall identify and appropriately secure areas of the network pertaining to the confidentiality, security and safety of staff and student against unauthorized access.

Access to the district's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all rules governing use of the system and shall agree in writing to comply with such regulations and guidelines.

Noncompliance with the applicable board policies and regulations may result in limitation, suspension, or termination of privileges and other disciplinary action. Violations may result in disciplinary action up to and including suspension or expulsion from campus and criminal prosecution as appropriate to the severity of the offense.

World Wide Web

All students and employees of the board shall have access to the Web through the district's networked or stand alone computers. An agreement shall not be required. To deny a child access, parents/ guardians must notify the building principal in writing.

Classroom E-mail Accounts

Students in grades K-8 shall be granted e-mail access through classroom accounts only. To deny a child access to a classroom account, parents/guardians must notify the building principal in writing.

INTERNET SAFETY TECHNOLOGY (continued)

Individual E-mail Accounts for Students

Students in grades K-8 may have individual accounts at the request of teachers and with the consent of parents/guardians. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian.

Individual E-mail Accounts for District Employees

District employees shall be provided with email access. Access to the system will be provided for staff members who have signed the acceptable use policy agreement. Email will be monitored and archived for three years. Employee email is discoverable and will be released if subpoenaed within the archival period set forth in this policy.

District Web Site

The board authorizes the chief school administrator to establish and maintain a district web site. The purpose of the web site will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish web sites that include information on the activities of that school or class. The building principal shall oversee these web sites.

The chief school administrator shall publish and disseminate guidelines on acceptable material for these web sites. The chief school administrator shall also ensure that district and school web sites do not disclose personally identifiable information about students without prior written consent from parents/guardians. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

Parental Notification and Responsibility

The chief school administrator shall ensure that parents/guardians are notified about the district network and the rules governing its use. Parents/guardians shall sign an agreement to allow their child(ren) to have an individual account. Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Acceptable Use

Student Safety Practices

Students shall not post personal contact information about themselves or others. Nor shall students engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities

Users shall not attempt to gain unauthorized access (hacking) to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

INTERNET SAFETY TECHNOLOGY (continued)

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

System Limits

Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet "chat room" conversations.

Users shall check e-mail frequently and delete messages promptly.

Privacy Rights

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

School Furnished Electronic Devices

The district may furnish students electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices. When a student is furnished with an electronic device the district

INTERNET SAFETY TECHNOLOGY (continued)

shall provide the student with written or electronic notification that the electronic device may record or collect information on the student's activity or the student's use of the device if the electronic device is equipped with a camera, global positioning system, or other feature capable of recording or collecting information on the student's activity or use of the device. The notification shall also include a statement that the district shall not use any of the capabilities in a manner that would violate the privacy rights of the student or any individual residing with the student. The parent or guardian of the student furnished an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgement as long as the student retains the use of the electronic device.

Failure to provide the required notification shall be subject to a fine of $250 per student, per incident. If imposed, the fine shall be remitted to the Department of Education, and shall be deposited in a fund that shall be used to provide laptop or other portable computer equipment to at-risk pupils.

Implementation

The chief school administrator may prepare regulations to implement this policy.

Adopted:	September 2001
NJSBA Review/Update:	February 2009
Readopted:	June 16, 20019
Revised & Readopted:	December 11, 2012
Revised & Readopted:	October 8, 2013
Revised & Readopted:	October 14, 2014

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Internet Safety, Technology, Web Site, World Wide Web, CIPA

Legal References:

N.J.S.A. 2A:38A-1 et seq.	Computer System
N.J.S.A. 2C:20-25	Computer Related Theft
N.J.S.A. 18A:7A-10	NJQSAC
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
N.J.S.A. 18A:36-39	Notification by school to certain persons using certain electronic devices; fine
N.J.A.C. 6A:30-1.1et seq.	Evaluation of the Performance of School Districts

17 U.S.C. 101 - United States Copyright Law

47 CFR 54.503(d) - Competitive Bidding; Gift Restrictions

47 U.S.C. 254(h) - Children's Internet Protection Act

State in re T.L.O., 94 N.J. 331 (1983), reversed on other grounds, New Jersey v. T.L.O., 569 U.S. 325 (1985).

O'Connor v. Ortega 480 U.S. 709 (1987)

No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

Possible Cross References:

*1111	District publications
*3514	Equipment
3543	Office services

INTERNET SAFETY TECHNOLOGY (continued)

*3570	District records and reports
4118.2/4218.2	Freedom of speech (staff)
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.1	Harassment, intimidation and bullying
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (students)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.

MILLTOWN BOARD OF EDUCATION **FILE CODE: 6142.10**
Milltown, New Jersey

Regulation

ACCEPTABLE USE REGULATIONS

A. Personal Responsibility: As a representative of the Milltown School District, I will accept personal responsibility for reporting any misuse of equipment or system access to the program administrator. Misuse may come in many forms, but it is commonly viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below.

B. Acceptable Use: The use of my assigned account must be in support of education and educational research, and in alignment with the educational goals and objectives of the Milltown School District. I am personally responsible for this provision at all times when using electronic information service.

1. Transmission of any material in violation of any United States or other state organizations is prohibited. This includes, but is not limited to copyrighted material threatening or obscene material.

2. Use of product advertisement or political lobbying is also prohibited.

C. Privileges: The use of the information system is a privilege, not a right. Inappropriate use will result in a cancellation of those privileges. The program administrator, in cooperation with the administrative team, will decide what is appropriate to use. The administration or staff of the Milltown School District may request that the program administrator revoke or suspend specific user access.

D. Network Regulations: These rules include, but are not limited to the following:

Student Safety Practices

Students shall not post personal contact information about themselves or others. Nor shall students engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities

Users shall not attempt to gain unauthorized access to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not purposely or maliciously destroy or deface equipment, peripherals or software.

Users shall not use the district system to engage in illegal activities as outlined in federal and state law and network provider policies and licenses.

Users shall not utilize third-party email accounts unless the purpose is for school related activities.

ACCEPTABLE USE REGULATIONS (continued)

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

User shall not vandalize the account, work or data of another user.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Users shall not utilize technology for the personal financial or business gain.

Users shall not install or use personal software or change the configuration of any individual computer or network.

User shall not utilize file sharing programs unless it is for school related activities.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

System Limits

Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet "chat room" conversations.

Users shall check e-mail frequently and delete messages promptly.

ACCEPTABLE USE REGULATIONS (continued)

Privacy Rights

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

Users shall be aware that electronic mail is not guaranteed to be private, particularly of there are reasonable grounds for suspecting that the search would turn up evidence that the user has violated or is violating either the law or rules of the school. Messages relating to or in support of illegal activities may be reported to the authorities.

E. Release of Information: Only the Webmaster of the Milltown Board of Education may select student work, pictures and/or names for approval by Chief school administrator to publish on the District web site.

F. Services: The Milltown School District makes no guarantees of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages suffered while on the system.

G. Vandalism: Vandalism is defined as any malicious attempt to harm or destroy hardware, data of another user or networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses. Any vandalism will result in the loss of computer services, disciplinary action, and legal referral.

F. Electronic Equipment: Cell phones, Iwatches, recording devices, radios, Ipods, and other solar, battery or electronic powered devices and equipment or the like, must be turned off during the school day and stored in lockers or backpacks.

What I need to know about US Copyright Act

A. It is illegal to copy or distribute software. If you have a legal copy of software you are allowed to make a single archival copy for backup purposes.

B. Copies of software licensed to the school district may be installed on your own personal home computer for educational purposes.

C. Staff owned software might be installed on his/her classroom computer if used only for educational purposes (only your classroom computer).

D. Establish and maintain a software inventory for your classroom computer.

E. Save purchasing documents and manuals for your software.

Milltown School District Guest Network Disclaimer

A. The wireless Internet access provided by the Milltown School District is provided on an "as is" and "as available" basis to authorized guests only. The Milltown School District does not warrant that this service will be uninterrupted, error-free, or free of viruses or other harmful components. Internet access at designated areas is provided only as a courtesy and may or may not be available at any requested time. Users should be aware that there are security, privacy, and confidentiality risks inherent in wireless communications and technology, and the Milltown School District does not make any assurances or warranties relating to such risks. No technical support of any kind under any circumstances will be provided to any user trying to access the wireless network, unless at the express direction of the Superintendent.

ACCEPTABLE USE REGULATIONS (continued)

B. By using wireless Internet access, users agree that the Milltown School District is not liable for any costs or damages arising from use of this service and Milltown School District does not control any materials, information, products or services on the Internet.

C. We reserve the right to deny or restrict access by any user if we suspect misuse of the network, or if the user has misused the network in the past. Misuse of the network shall be determined solely by the Milltown School District and shall include, but not be limited to, any inappropriate activity, excessive bandwidth consumption, unnecessary use, exposing the network to viruses or malware, recreational use, and/or illegal activity.

Milltown School District Guest Network User Assurances

A. I will not utilize the network to participate in any illegal activity and/or any type of hacking activities. I will not use any device to take pictures or video of anyone on school property or post or send any pictures or video without authorization from Milltown School District. I understand that the school district is required by law to have a filter on the Internet and will not use my device to access content that would otherwise be inaccessible through the Internet filter utilized by the Milltown School District. I will not attach any device of any kind to the district's wired network. While using the network, I will not use someone else's intellectual property without their written permission.

B. I understand that I am solely responsible for my own electronic devices. The Milltown School District bears no obligation to allow me to charge any devices. I understand that I will not be permitted to access network folders or access and utilize school printers. I understand that the Milltown School District can inspect my personal devices for any reason, and that the Milltown School District is not responsible for the security, repair, troubleshooting, technical support, loss, misplacement, theft, or damage to any of my personal electronic devices, or any other property arising from the use of the Milltown School District guest network.

Revised: March, 2013
Adopted: December 11, 2012
Revised: August 21, 2001
Readopted: October 14, 2014