Merchantville Board of Education 130 South Centre Street Merchantville, NJ 08109	File Code : 6142.10 Proposed : 09/22/2009 Adopted : 10/13/1009 Revised : 04/25/2017 Reviewed : 07/15/2024

Technology

The board 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 New Jersey Student Learning 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).

The district shall ensure equal and bias-free access for all students to computers, computer classes, career and technical education programs, and technologically-advanced instructional assistance, regardless of race, creed, color, national origin, ancestry, age, marital status, affectional/sexual orientation, gender, religion, disability, English proficiency, immigration status, housing status or socioeconomic status.

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 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 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 lead person or his or her designee.

The lead person 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 school 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 school 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 board 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 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.

The chief school administrator shall coordinate the district system by approving all activities for the district; 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.

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.

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 be required. To deny a child access, parents/ guardians must notify the chief school administrator 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 chief school administrator in writing.

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. This account will not include remote access.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual account and remote access to the system. An agreement shall be required.

Supervision of Students

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

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.

Classes may also establish Web sites that include information on the activities of that class. The chief school administrator 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 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 chief school administrator 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 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 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 school 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 school 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 school 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 school 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 shall prepare regulations to implement this policy.

Key Words

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

Legal References

N.J.S.A. 2A 38A-1: Definitions
N.J.S.A. 2C 20-25: Computer criminal activity; degree of crime; sentencing.
N.J.S.A. 18A 7A-10 et seq: New Jersey Quality Single Accountability Continuum for evaluating school performance.

N.J.S.A. 18A 36-35 Disclosure of certain student information on Internet prohibited without parental consent
N.J.S.A. 18A 36-39 Notification by school to certain persons using certain electronic devices; fine.
N.J.A.C. 6A 30-1.1 Purpose and scope
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
New Jersey v. T.L.O.
O'Connor v. Ortega
20 U.S.C. 6301 et seq Every Student Succeeds Act (Formerly NCLB)

Cross References

1111 - Sample Policy: District Publications
3514 - Sample Policy: Equipment
3570 - Sample Policy: District Records and Reports
5114 - Sample Policy: Suspension and Expulsion
5124 - Sample Policy: Reporting to Parents Guardians
5131 - Sample Policy: Conduct and Discipline
5131.5 - Sample Policy: Vandalism Violence
5142 - Sample Policy: Pupil Safety
6144 - Sample Policy: Controversial Issues
6145.3 - Sample Policy: Publications

NJSBA File Date: 05/06