



Book	Policy Manual
Section	Series 6000 Instruction
Title	Internet Safety and Technology
Number	6142.10
Status	Second Reading
Adopted	October 17, 2013
Last Reviewed	May 31, 2018

### **BRICK TOWNSHIP BOARD OF EDUCATION Policy**

X	Monitored
X	Mandated
X	Other Reasons

#### INTERNET SAFETY AND TECHNOLOGY

The Brick Township 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 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 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 superintendent or his or her designee.

The superintendent 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. Cyber bullying (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 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 superintendent 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.

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.

#### 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 building principal in writing.

#### Individual Email 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 Network and Website

Students, staff and administration of the school district shall have the opportunity to access the Internet to facilitate the need to prepare students, staff and administrators to become computer literate in an increasingly technological world, to foster educational and personal growth in technology, information gathering, and communication skills. It is understood that the school district does not have sufficient staff to monitor every aspect of the use of the Internet.

However, the district will foster the independent use of the school's network, subject to compliance with procedures and standards for appropriate network behavior and communication. The following guidelines shall apply to all users when accessing any school district network connection (NET):

- A. The primary use of the NET shall be reserved to those individuals who utilize the materials that are of "educational value" to students of the district. For purposes of these guidelines, "educational value" shall mean those areas of network access that have a direct or indirect impact on the students' educational program in the school district. The use of the system for defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, and racially offensive, and illegal material or other prohibited activities shall not be permitted, and the school district will use any and all means available to it, within the confines of the law to prevent such material from entering the NET. Individuals are encouraged to report such entry of material into the system to the building administrator;
- B. No personnel or student information that is protected by the Family Educational Rights and Privacy Acts shall be disseminated through the NET;
- C. All users of the NET must comply with the Electronic Communications Privacy Act of 1986, as amended, and the Communications Decency Act. These Acts prohibit the unauthorized interception or disclosure of email messages by third parties, as well as the appropriateness of certain material being remitted on the Internet. The Acts do not permit interception or disclosure unless both the sender and the receiver of the communication consent. Further, the Acts recognize that the school district may monitor an employee's email messages, as long as the interception device is included in the email equipment;
- D. Users of the NET must recognize that the district administration does have the authority to intercept email messages of all users and that there will be no privacy right construed by the district to exist in the statements made in the NET. Users of the NET are encouraged not to store extensive email messages in the NET and that

messages should be stored for a period of no longer than 14 calendar days;

- E. When issued individual passwords and accounts, NET users may not allow any other persons to use or share those passwords and/or accounts;
- F. Any attempt to circumvent system security, guess passwords, or in any way gain unauthorized access to local or NET resources is forbidden;
- G. Use of the Internet for political and/or commercial gain or profit is not allowed from an educational site;
- H. Users may not move, repair, reconfigure, modify or attach external devices to the system;
- I. Additional rules and restrictions may be added and users will be notified of these changes in a timely manner. Users are responsible for reading and following these rules;
- J. Time restrictions on the use of the Internet may be imposed to ensure equity of use;
- K. From time to time, the district will encourage students and employees to use certain informational sources in order to control internet costs;
- L. The district administration reserves the right to use electronic devices, cards, or any other media to determine whether or not the students or employees are using the NET for items of true educational value;
- M. Professional employees of the school will monitor student use of the Internet.

Students or employees who violate the internet guidelines of the school may be denied future internet privileges for a defined period of time or other disciplinary measures set forth in the student code of conduct or in any other rules of the district that may be applicable.

#### Parental Notification and Responsibility

The superintendent 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.

#### 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.

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.

#### Cyber bullying

The board of education expressly forbids cyber bullying. For the purposes of this policy, "cyber bullying" shall mean using the communication capacities of computers, the Internet and/or other digital communication devices to bully others by:

- A. Sending or posting cruel messages or images;
- B. Threatening others;
- C. Excluding or attempting to exclude others from activities or organizations;
- D. Starting or passing on rumors about others or the school system;
- E. Harassing or intimidating others;
- F. Sending angry, rude or vulgar messages directed at a person or persons privately or to an online group;
- G. Sending or posting harmful, untrue or cruel statements about a person to others;
- H. Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger;
- I. Sending or posting material about a person that contains sensitive, private or embarrassing information, including forwarding private messages or images; and/or
- J. Engaging in tricks to solicit embarrassing information that is then made public.

Students found to be engaging in activities as describe above shall be subject to the terms and sanctions found in this policy and board policies 5131.1 Harassment, Intimidation and Bullying and 5131 Conduct and Discipline.

#### 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 email 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 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 superintendent may prepare regulations to implement this policy.

Key Words

Acceptable Use, Blocking/Filtering Software, Email, Internet, Internet Safety, Technology, Website, World Wide Web, CIPA

**SEE ATTACHED:****PARENT/GUARDIAN AGREEMENT REGARDING THE USE OF DISTRICT-OWNED ELECTRONIC DEVICES**

Legal	<a href="#">N.J.S.A. 2A 38A-1: Definitions</a>
	<a href="#">N.J.S.A. 2C 20-25: Computer criminal activity; degree of crime; sentencing.</a>
	<a href="#">N.J.S.A. 18A 7A-10 et seq: New Jersey Quality Single Accountability Continuum for evaluating school performance.</a>
	<a href="#">N.J.S.A. 18A 36-35 Disclosure of certain student information on Internet prohibited without parental consent</a>
	<a href="#">N.J.S.A. 18A 36-39 Notification by school to certain persons using certain electronic devices; fine.</a>
	<a href="#">N.J.A.C. 6A 30-1.1 Purpose and scope</a>
	<a href="#">17 U.S.C. 101 United States Copyright Law</a>
	<a href="#">47 CFR 54.503(d) Competitive Bidding; Gift Restrictions</a>
	<a href="#">47 U.S.C. 254(h) Children's Internet Protection Act</a>
	<a href="#">New Jersey v. T.L.O.</a>
	<a href="#">O'Connor v. Ortega</a>
	<a href="#">20 U.S.C. 6301 et seq Every Student Succeeds Act (Formerly NCLB)</a>



[6142.10 Internet Safety and Technology\\_Parent Notification Form.pdf \(15 KB\)](#)

Last Modified by Sandra Beyer on July 11, 2018

