

FILE 6142.10 INTERNET SAFETY AND TECHNOLOGY

The Rahway 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 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 the Internet, email, or other forms of direct electronic communication;
- 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 student access to inappropriate information by way of the Internet or other forms of electronic communication.

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 district's online computer network when using email, chat rooms, instant messaging, and other forms of direct electronic communication.

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 district staff to educate, supervise, and monitor usage of the 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 designee.

The superintendent or 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 networking websites, and chat rooms;
- D. Cyberbullying awareness and response (Board Policy 5131.1 Harassment, Intimidation, and Bullying).

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 provide 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 or she shall recommend to the board 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 or 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 policy and regulations 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 standalone computers. A signed agreement shall be required of both employees and students; student use shall also require the signature of a parent/guardian. To deny a child access, parents/ guardians must notify the building principal in writing.

Individual Email Accounts for Students

Students in grades 4-12 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 or her parent/guardian.

Students in grades 9-12 may be granted individual email accounts and access to the network. An agreement shall be required for an individual email account and must be signed by the student and his or her parent/guardian.

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/School Websites

The board authorizes the superintendent to establish and maintain a district website. The purpose of the website will be to inform the district educational community of district programs, policies, and practices.

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

The superintendent shall publish and disseminate guidelines on acceptable material for these websites. The superintendent shall also ensure that district and school websites 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 New Jersey Department of Education. "Personally identifiable information" refers to student names, photos, addresses, email addresses, phone numbers, and locations and times of class trips.

Parent/Guardian 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 online. 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 access 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," trapdoor program codes, spyware, malware, 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 webpages.

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 or her password to another individual.

Users shall immediately notify the supervising staff person or technology administrator 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 email 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/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 laptops or other portable computer equipment to at-risk students.

Privately Owned Electronic Devices

The use of privately owned electronic devices by district employees during the performance of their duties must be approved by the appropriate administrator beforehand. The district shall not be responsible for loss of or damage to any personally owned technology devices that students and employees bring to school. Such damage or loss shall be the responsibility of the owner of the device, who shall also bear responsibility for insuring the device, if desired.

Implementation

The superintendent may prepare regulations to implement this policy.

Adopted: September 15, 1998

Revised: April 24, 2001

Revised: January 15, 2008

NJSBA Review/Update: May 2016

Readopted: December 20, 2016

Revised: August 22, 2017

Revised: October 16, 2018

Key Words

Acceptable Use, Blocking/Filtering Software, Email, Internet, Internet Safety, Technology, Website, 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:30-1.1](#) *et 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)

Every Student Succeeds Act of 2015, [Pub.L. 114-95](#), [20 U.S.C.A. 6301](#) *et seq.*

Possible Cross References:

*1111 District publications

*3514 Equipment

3514.1 Bring your own device (BYOD)

3543 Office services

*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 Student 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.

Rahway Public Schools