

<input checked="" type="checkbox"/>	Monitored
<input checked="" type="checkbox"/>	Mandated
<input checked="" type="checkbox"/>	Other Reasons

## Policy

### ATTENDANCE, ABSENCES, AND EXCUSES

The board of education believes that the regular attendance of students in each class and in school in general is critical to its educational mission. The district shall endeavor to achieve the ninety percent (90%) attendance rate required by the New Jersey Quality Single Accountability Continuum (NJQSAC). Continuity of instruction is an essential element in student performance and allows students the greatest opportunity to succeed at meeting the state learning standards in the Core Curriculum Content Standards. The chief school administrator shall oversee the development of effective strategies that maximize student attendance at all scheduled periods of actual instruction or supervised study activities and strive to:

1. Encourage good attendance;
2. Discourage unexcused absences;
3. Identify patterns of absence, tardiness and early departures from school; and
4. Intervene to prevent and correct problems with attendance.

#### Definitions

"Attendance" is a student's presence in school and in the classroom to which he or she is assigned at the times scheduled for instruction or other school activities. A school day shall consist of not less than four hours of actual instruction. An approved kindergarten school day shall consist of one continuous session of at least 2 1/2 hours may be considered as a full day.

The mere presence of a student at roll call shall not be regarded as sufficient to be considered in attendance for a school day. A student shall be present at least one hour during both the forenoon and the afternoon in order to be recorded as present for the full day. In a school which is in session during either the forenoon or the afternoon, a student shall be present at least two hours in the session in order to be recorded as present for the full day.

A student not present in school because of his or her participation in an approved school activity, such as a field trip, meeting, cooperative education assignment, or athletic competition will be considered to be in attendance.

"Excused absence" is a student's absence from school for a full day or a portion of a day for one or more of the following reasons:

1. The student's illness;
2. \*Requirements of a student's individual health care plan;
3. A death or critical illness in the student's immediate family, or others with permission of principal;
4. Quarantine;
5. \*Observance of the student's religion on a day approved for that purpose by the State Board of Education;
6. The student's suspension from school;
7. \*Requirements of the student's Individualized Education Program (IEP);
8. \*Alternate short or long term accommodations for students with disabilities;
9. The student's required attendance in court;
10. Interviews with an admissions officer of an educational institution;
11. Necessary and unavoidable medical or dental appointments that cannot be scheduled at a time other than the school day;
12. Such good cause as may be acceptable to the principal.

#### \*Mandated

Attendance need not always be within the school facilities. A pupil will be considered to be in attendance if he/she is present at any place where school is in session by authority of the board. The board shall consider each pupil assigned to a program of independent study, with parent/guardian permission, to be in regular attendance for that program, provided that he/she is under the guidance of a staff member so assigned, reports daily or weekly, as prescribed, to such staff member the place in which he/she is conducting his/her study, and regularly demonstrates progress toward the objectives of his/her course of study.

"Unexcused absence" is a student's absence for all or part of a school day for any reason other than those listed in paragraph "Excused Absences" above. Absence is expressly not excused for any of the following purposes (this list is intended to be illustrative and is not inclusive):

INTERNET SAFETY AND 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.

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.

**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.

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:

INTERNET SAFETY AND TECHNOLOGY (continued)

- 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.

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.

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.

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.

INTERNET SAFETY AND TECHNOLOGY (continued)

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

INTERNET SAFETY AND TECHNOLOGY (continued)

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.

Implementation

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

First Reading:

Second Reading:

Mandated:

47 U.S.C. 254(h), known as the Children's Internet Protection Act (CIPA) and the implementing federal regulations, require board policy on acceptable use of the Internet for districts receiving certain federal funds, as well as the installation of blocking software to prevent access to unacceptable areas of the Internet.

The Children's Internet Protection Act is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA.

What CIPA Requires:

- A. Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal;
- B. Schools subject to CIPA are required to adopt and enforce a policy to monitor online activities of minors;
- C. Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.

An eligible school or library may not directly or indirectly solicit or accept any gift, gratuity, favor, entertainment, loan, or any other thing of value from a service provider participating in or seeking to participate in the schools and libraries universal service program. Gift prohibitions are applicable year-round, not just during the competitive bidding process. This prohibition includes an applicant soliciting and receiving any gift or other thing of value from an E-rate service provider.

47 CFR § 54.503(d) of the federal competitive bidding regulations restricts district personnel, board members and contracted service providers from receiving gifts from vendors in excess of \$20.00 for any single item such as meals, pencils, pens, hats, t-shirts etc. Total gifts received by any individual during a one year period

**INTERNET SAFETY AND TECHNOLOGY** (continued)

from any one vendor shall not exceed \$50.00. These restrictions apply to any employee, board member or contracted service provider of a district that participates in the Schools and Libraries Program of the Universal Service Fund (E-rate Program). Failure to comply is a violation of FCC rules and will result in expulsion from the E-rate program.

No Child Left Behind also requires policy on safe student access to the Internet.

**Other Reasons:**

N.J.S.A. 18A:36-35 prohibits the publication on district web sites of "personally identifiable information" about students without prior written parental consent. "Personally identifiable information" is defined as student names, photos, addresses, email addresses, phone numbers and locations and times of class trips.

This is a topic of critical concern, because technology has important implications for all aspects of district operations.

**Recommendation:**

A policy directing the development of a technology plan that effectively integrates technology into district programs, practices and operations. The policy should include a section on the entire system of electronic communications and whatever other sections apply to your district system – acceptable use of the Internet, web sites, e-mail for staff and/or students, district rights and responsibilities, parental responsibilities, etc. Include assurances of the installation of blocking software if your district receives E-rate discounts for Internet access or federal funds for some other technological uses. According to federal law, filters should block visual depictions that are obscene, child pornography, or harmful to minors. All forms of "hacking" should be prohibited. Assure monitoring of student online activities.

Sanctions for student misuse of the system should be included in your student code of conduct or regulations for policy 5131 Conduct/Discipline. Sanctions for staff misuse would be addressed in negotiated agreements and applicable laws and regulations. List other related policies in your cross references.

<b><u>Legal References:</u></b>	<u>N.J.S.A.</u> 2A:38A-1 <u>et seq.</u>	Computer System
	<u>N.J.S.A.</u> 2C:20-25	Computer Related Theft
	<u>N.J.S.A.</u> 18A:7A-10 <u>et seq.</u>	New Jersey Quality Single Accountability Continuum for evaluating school performance
	<u>N.J.S.A.</u> 18A:36-35	School Internet websites; disclosure of certain student information prohibited
	<u>N.J.A.C.</u> 6A:30-1.1 <u>et seq.</u>	Evaluation of the Performance of School Districts
	17 <u>U.S.C.</u> 101	United States Copyright Law
	47 <u>CFR</u> 54.503(d)	<u>Competitive Bidding; Gift Restrictions</u>
	47 <u>U.S.C.</u> 254(h)	<u>Children's Internet Protection Act</u>
	<u>State in re T.L.O.</u> , 94 <u>N.J.</u> 331 (1983), reversed on other grounds, <u>New Jersey v. T.L.O.</u> , 569 <u>U.S.</u> 325 (1985).	
	<u>O'Connor v. Ortega</u> , 480 <u>U.S.</u> 709 (1987)	
	<u>No Child Left Behind Act of 2001</u> , PL 107-110, 20 <u>U.S.C.A.</u> 6301 <u>et seq.</u>	