



CONSOLIDATED SCHOOL DISTRICT OF NEW BRITAIN

Board Policy Statement

6141.32 - Access to Internet

Approved on April 15, 2002

The Board of Education supports the use of electronic information systems to improve learning, teaching and managing. These systems enhance student access to information, research, teacher training, collaboration and dissemination of successful educational practices, methods and materials. The school system's connection to the Internet provides access to local, national and international sources of information and collaboration vital to intellectual inquiry in a democracy.

Every electronic information systems user within this school system has the responsibility to respect and protect the rights of every other user in our school community and on the Internet. Each user must use these systems in a responsible, ethical and legal manner in accordance with this policy and administrative procedure, as well as state and federal law.

This policy and administrative procedure applies to supervised and independent uses of all forms of technology. It does not attempt to articulate all access scenarios and user behaviors. All users will be required to sign and comply with the District's Electronic Information Systems Use Agreement. Violation of this policy and administrative procedure will result in appropriate consequences, which may include disciplinary measures and legal action.

Legal References/Citations

Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. 1232g

Conn. Gen. Statute Section 31-48d

U.S. Department of Education Regulations, 34 C.F.R. Part 99

Children's Internet Protection Act of 2000, 20 U.S.C. 6801, et. seq.

Communications Act of 1934, as amended, 47 U.S.C. 254 (h) and (l)



CONSOLIDATED SCHOOL DISTRICT OF NEW BRITAIN

Administrative Procedure

6141.32 - Access to Internet

Approved on April 15, 2002 | Revised July 2020

I. Purpose

The purpose of these procedures is to establish guidelines for the proper use of the School District's Computer Networks and Electronic Information Systems, consistent with state and federal law.

II. Definitions

For purposes of these procedures, the following terminology will apply:

- A. Information system is any configuration of hardware and software that provides users access to information stored electronically. The configuration can be a single unit or multiple units networked together. It includes the E-mail system and the Internet.
- B. Networks include computer hardware, operating system software, application software, and stored text and data files, regardless of source and content.
- C. User includes any person who has authorization to utilize the School District's information systems or networks, including students and employees. It may also include other persons outside of these groups who have authorization to use District facilities and in the course of using District facilities require access to the systems.

III. Ownership/Electronic Monitoring

The information systems and networks are the property of the Board of Education and are provided for the purpose of carrying out the educational and operational needs of the School District.

Use of the School District's information systems and networks is not guaranteed to be private, and users do not have an expectation of privacy in their use of these systems.

The School District reserves the right to monitor the use of such systems, including but not limited to, E-mail in order to ensure compliance with its guidelines by, for example, bypassing passwords. Users consent to allowing the school system to access and review all materials users create, store, send or receive on the computer system or through the Internet or any other computer network or information systems.

IV. Acceptable/Unacceptable Uses; Reporting

A. Acceptable uses

The School District's information systems and networks may be used (1) to further the Board of Education's goals; (2) to support education and research; (3) for school-related communications; or (4) other legitimate school business.

B. Unacceptable uses

The following actions and activities are prohibited on any of the School District's information systems and networks:

- a. Engaging in any illegal activity, including violation of software licenses, contracts, or transmitting any material in violation of federal or state law.
- b. Unauthorized downloading of software, regardless of whether it is copyrighted or devised.
- c. Downloading copyrighted material for other than personal use.
- d. Using the network or information systems for private, financial, or commercial gain.
- e. Wastefully using resources, such as file space.
- f. Hacking or gaining unauthorized access to files, resources, or entities.
- g. Invading the privacy of individuals, which includes the unauthorized access to, or dissemination of, information about anyone that is of a highly personal nature.
- h. Using another user's account or password.
- i. Posting material authorized or created by another without his/her consent.
- j. Posting anonymous messages.
- k. Accessing, submitting, posting, publishing, or displaying any defamatory, fraudulent, abusive, obscene, profane, sexually explicit, intimidating, threatening, racially offensive, harassing, or illegal material.
- l. Accessing or disclosing confidential information about a student or from a student's school records without proper authorization. (See Board Policy 3-9).
- m. Unauthorized bypassing of filtering software or knowingly visiting inappropriate websites.
- n. Unauthorized bypassing of security software.
- o. Altering the attribution-of-origin information in E-mail communications.
- p. Providing copies of School District software to individuals outside the School District without proper authorization.

- q. Installing, removing, revising, or adapting software without proper authorization.
- r. Using the networks or information systems in a manner that conflicts or interferes with an employee's job duties, work performance, professional responsibilities.
- s. Using the networks or information systems in a manner that violates any Board of Education policies.
- t. Student action and activities in violation of Guidelines for Social Media and Cyber Bullying (see Part IV – Section D)

Note: The above list is not all inclusive of each and every use that may be deemed unacceptable.

C. Reporting

Any individual who receives any inappropriate material on the School District's networks or information systems should immediately report the incident to a teacher or administrator as appropriate. Any individual who becomes aware of any use of the networks or information systems in violation of this policy should immediately report the incident to a teacher or administrator as appropriate.

D. Guidelines for Social Media and Cyber Bullying

The New Britain Board of Education recognizes the importance of social media for its employees and acknowledges that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern.

The Board of Education also recognizes that inappropriate content created by employees can be disruptive to the educational environment, violate the Board's responsibilities regarding confidential information, and compromise the goodwill and reputation of the school district.

Therefore, Board of Education employees may be subject to disciplinary action (up to and including termination) when their personal use of social media does any of the following:

- Disrupts the operations of the school district.
- Interferes with the educational process.
- Breaches the confidentiality rights of students or employees.
- Harasses co-workers or other members of the school community.
- Creates a discriminatory or hostile working or learning environment.
- Endangers or otherwise puts students at risk of harm.
- Harms the goodwill and reputation of the school district in the community.
- Violates the law, board policies, or other school rules and regulations.

The term "social media" refers to online social interaction or other public display of personal information via electronic means. Current examples of social media include, but is not limited to Facebook, Twitter, LinkedIn, Snapchat, TikTok, YouTube, and other media platforms. The term "Board of Education" includes all names, logos, buildings, images, and entities under the authority of the New Britain Board of Education.

The Board of Education also recognizes that inappropriate content created by students can be disruptive to the educational environment and can violate the rights of other students and their right to privacy. Therefore, students may be subject to disciplinary action (up to and including loss of all computer privileges) when their personal use of social media does any of the following:

- Disrupts the operations of the school district.
- Interferes with the educational process.
- Breaches the confidentiality rights of students or employees.
- Harasses classmates or other members of the school communities.
- Creates a discriminatory or hostile learning environment.
- Endangers or otherwise puts students at risk or harm.
- Violates the law or any of the Board's policies or regulations.

V. Internet Safety/Filters

A. General warning/Individual responsibility

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an E-mail address on the Internet may lead to receipt of unsolicited E-mail containing offensive content. Users accessing the Internet do so at their own risk. The School District is not responsible for material viewed or downloaded by users from the Internet.

The Internet changes rapidly making it impossible to filter all objectionable sites. Therefore, the teaching staff must supervise and monitor student access to the Internet. In addition, each individual has the responsibility to monitor his/her own navigation on the Internet to avoid undesirable sites.

In order for the School District to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the school's teachers and other staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged students.

In recognizing the importance of public education and outreach in regards to internet safety and cyber bullying, the Board of Education will hold a public informational forum on the internet safety and cyber bullying to the public on a yearly basis.

B. Filters

The School District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornographic, or (3) harmful or inappropriate for minors as determined by the superintendent or his/her designee(s). The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material, which is inappropriate for minors.

Filters will be used with District schools to (1) block pre-selected sites; (2) block by word; (3) block entire categories like chat and newsgroups; and (4) through a pre-selected list of approved sites.

Filtering should only be viewed as one of a number of techniques used to manage student's access to the Internet and encourage acceptable usage. It should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors.

C. Disabling blocking/filtering devices

An administrator, teacher or supervisor may submit a request to the Superintendent or his/her designee to have an Internet filtering system be disabled or a site unblocked, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 18 or older.

VI. Authorization for Access to the Electronic Networks and Information Systems

Authorized access to the information systems and networks shall be given only to those individuals who agree to use these systems in a responsible manner and agree to comply with Board policies and procedures. Use of computer resources is a privilege that may be revoked if it is misused or abused.

- A. Use of computer networks and information systems shall be restricted to individuals who have signed the "Acceptable Use and Internet Access Agreement" (Appendix A)
- B. Student network accounts will only receive internet and cloud based account access upon completion of internet safety and cyber bullying training.

APPENDIX A

ELECTRONIC INFORMATION SYSTEMS USE AND INTERNET ACCESS AGREEMENT

Students, parent(s)/guardian(s), and staff members need only sign this agreement once while enrolled or employed by the School District.

I have read, understand, and agree to abide by the terms of Board Policy 6141.32 and Administrative Procedures. Should I commit any violation or in any way misuse my access to the School District's computer networks or information systems, I understand and agree that my access privilege may be revoked and disciplinary action may be taken against me.

In consideration for using the School District's electronic networks and information systems, I hereby release the School District and its employees, acting in the scope of their employment, from any claims and damages arising from my use of the Internet or E-mail.

User's name (print clearly) _____

User's signature: _____ Date: _____

Status: Student _____ Employee _____

I am 18 or older _____ I am under 18 _____

If I am signing this policy when I am under 18, I understand that when I turn 18 this policy will continue to be in full force and effect and agree to abide by this policy.

Parent/Guardian: (If applicant is under 18 years of age, a parent or guardian must also read and sign this agreement). As the parent or legal guardian of the above student, I have read, understand and agree that my child or ward shall comply with the terms of the School District's Acceptable Use and Internet Safety policy and procedures for the student's access to the School District's computer networks and information systems. I understand that access is being provided to the students for educational purposes only.

However, I also understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by this policy. I am, therefore, signing this policy and agree to indemnify and hold harmless the school, the School District, and its employees acting in the scope of their employment against all claims, damages, losses, and costs, of whatever kind that may result from my child's or ward's use of his/her access to such networks or his/her violation of the foregoing policy.

Further, I accept full responsibility for supervision of my child's or ward's use of his/her access account if and when such access is not in the school setting. I hereby give permission for my child or ward to access the School District's computer networks and the Internet.

Parent/Guardian (please print): _____

Signature: _____ Date: _____