TRENTON BOARD OF EDUCATION
POLICY

FILE CODE: 6142.10

X Monitored
X Mandated
X Other Reasons

TECHNOLOGY

The Trenton Board of Education believes that technology should be infused into all areas of the curriculum and school operations. The Board believes that it is essential for the school district to bridge the digital divide that exists in urban areas as compared to the rest of the nation. The chief school administrator shall develop a technology plan that effectively uses electronic communication to advance and promote teaching and learning. This system of technology shall be used to provide local, statewide, national and global communications opportunities for staff and students. Educational technology shall be integrated into the district curriculum to maximize student achievement of the New Jersey Core Curriculum Content Standards.

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 administrator 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 determine that:

1. Access by minors to inappropriate matter on the Internet and the Web is restricted;
2. The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications is protected;
3. Unauthorized access, including so-called hacking and other unlawful activities by minors online does not occur;
4. Unauthorized disclosure, use and dissemination of personal identification information of minors does not occur and
5. Measures designed to restrict minors access to materials harmful to them are put in place.

The chief school administrator will be responsible to verify that blocking or filtering technology is implemented on all computers with Internet access. The blocking or filtering must protect against access to visual depictions that are obscene, pornographic, and violent and/or any materials harmful to minors.

School Staff Notification and Responsibility

Each principal shall coordinate the district's system in his/her building by approving all activities for that building;

ensuring that staff 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.

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.

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 computers.

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.

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

USE OF E-MAIL

Classroom and Individual E-mail Accounts for Students

Students may be granted classroom and individual e-mail accounts for educational purposes only. If e-mail accounts for students are requested as part of the instructional program, then that use will be monitored by the teacher responsible for that instructional program.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual account and access to the system.

SUPERVISION OF INTERNET

Supervision of Students

Student use of the Internet shall be supervised by staff.

ACCEPTABLE USE BY STUDENTS AND STAFF

Student Safety Practices

Students shall not have access to inappropriate matter or content on the Internet and the Web. 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. Any form of direct electronic communication by students (chatting, instant messaging, email) shall be monitored by staff or otherwise restricted from access.

Prohibited Activities

Staff and students shall not engage in any type of unauthorized access, including so-called "hacking," and other unlawful activities.

Staff and students 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.

Staff and students 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.

Staff and students shall not use the district system to engage in illegal activities, to conduct commercial activities, to advertise products or services or for political lobbying.

Staff and students 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.

Staff and students shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Staff and students shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Staff and students shall not assume the identity or use the password or materials of another person.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Staff and students shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Staff and students shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Staff and students 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.

Staff and students shall immediately notify the supervising staff person or technology office if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Staff and students shall not install or download software or other applications without permission of the supervising staff person.

Staff and students shall follow all district virus protection procedures when installing or downloading approved software.

System Limits

Staff and students shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists.

Staff and students shall check e-mail frequently and delete messages promptly.

Privacy Rights

Staff and students shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Staff and students shall not publish private information about another individual.

Implementation

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