TECHNOLOGY

The Harrison 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 pupils. Educational technology shall be infused into the district curriculum to maximize pupil achievement of the 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 pupils 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 pupils 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

Internet access in the Harrison School District is a privilege and not a right. Violating any of the guidelines or prohibitions listed in this policy can result in restricted network access, losing all network access privileges, and disciplinary or legal action including, but not limited to, criminal prosecution under appropriate local, state and federal laws. The systems administrator will close an account and/or restrict network access if necessary. An administrator or faculty member has the right to request, for cause, that the systems administrator deny, revoke or suspend specific user access or accounts.

This acceptable use policy shall govern all use of the system. Sanctions for pupil misuse of the system shall be included in the disciplinary code for pupils, as set out in regulations for policy 5131 Conduct/discipline.

TECHNOLOGY (continued)

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 pupils 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 E-mail Accounts for District Employees

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

Supervision of Pupils

Pupil use of the Internet shall be supervised by qualified staff.

District Web Site

The board authorizes the superintendent 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.

The superintendent shall publish and disseminate guidelines on acceptable material for these web sites. The superintendent shall also ensure that district and school web sites do not disclose personally identifiable information about pupils without prior written consent from parents/guardians. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to pupil names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

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.

Acceptable Use

Pupil Safety Practices

Pupils shall not post personal contact information about themselves or others. Nor shall pupils 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

TECHNOLOGY (continued)

Users 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.

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

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 superintendent shall prepare regulations to implement this policy.

Adopted: May 16, 2006
NJSBA Review/Update: June 2010
Readopted:

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web

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-11	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain pupil information prohibited
N.J.A.C. 6A:30-1.1et seq.	Evaluation of the Performance of School Districts
17 U.S.C. 101	United States Copyright Law
47 U.S.C. 254(h)	Children's Internet Protection Act
N.J. v. T.L.O. 469 U.S. 325 (1985)	
O'Connor v. Ortega 480 U.S. 709 (1987)	
No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.	

Possible Cross References:

*1111	District publications
*3514	Equipment
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
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (pupils)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.