

WINFIELD TOWNSHIP SCHOOL
7-1/2 GULFSTREAM AVENUE
WINFIELD, NEW JERSEY 07036

POLICY

FILE CODE: 6142.10

TECHNOLOGY

The Board 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 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 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. The Chief

School Administrator shall be responsible for maintaining a list of all passwords for all computers within the district. The Chief School Administrator shall designate those who have the ability to change passwords. All changed passwords must be updated on the master list.

The Chief School Administrator/Principal shall coordinate the district system by approving all activities for the 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 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. Parents, students and employees shall be given a copy of this policy and Acceptable Use of Computer Network/Computers and Resources (attached). After reading the policy parents, students and employees shall be required to sign an Internet Permission Form in order to gain access to the district computers and network. To deny a child access, parents/guardians must notify the building principal in writing.

Classroom E-mail Accounts

Students in grades K-8 shall be granted e-mail access through classroom accounts only. To deny a child access to a classroom account, 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 within the building. District employees shall be given a copy of this policy and Acceptable Use of Computer Network/Computers and Resources (attached). After reading the policy the staff member shall be required to sign an Internet Permission Form

in order to gain access to the district computers and network.

Supervision of Students

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

District Web Site

The Board authorizes the Chief School Administrator/Principal 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 Chief School Administrator/Principal shall oversee these web sites.

The Chief School Administrator/Principal shall publish and disseminate guidelines on acceptable material for these web sites. The Chief School Administrator/Principal shall also ensure that district and school web sites do not disclose personally identifiable information about students.. "Personally identifiable information" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips. Student photos, names, initials or any other personally identifiable information may not be posted on any district, school or class website.

Parental Notification and Responsibility

The Chief School Administrator/Principal 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 Chief School Administrator/Principal in writing.

ACCEPTABLE USE

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 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

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 shall prepare regulations to implement this policy.

Key Words

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

Legal References:

<u>N.J.S.A.</u> 2A:38A-1 <i>et seq.</i>	Computer System
<u>N.J.S.A.</u> 2C:20-25	Computer Related Theft
<u>N.J.S.A.</u> 18A:7A-11	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
<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:10A-1.1 <i>et seq</i>	Improving Standards-Driven Instruction and Literacy and Increasing Efficiency in Abbott

School Districts

See particularly:

N.J.A.C. 6A:10A, Appendix A

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 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.

Manual for the Evaluation of Local School Districts

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 (students)
6144	Controversial issues
6145.3	Publications
6161	Equipment, books and materials

Date: September 18, 2007

WINFIELD BOARD OF EDUCATION

ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES

File: 2361

GENERAL POLICY STATEMENT

The Board recognizes that as telecommunications and other new technologies shift the manner in which information is accessed, communicated and transferred that those changes alter the nature of teaching and learning. Access to new modes of telecommunication allows citizens and school employees to explore databases, libraries, Internet sites, bulletin boards and the like, while exchanging information with individuals throughout the world. The Board supports access by citizens and school employees to these new information sources, but reserves the right to limit in-school use of these materials and modes of communication to subjects and areas that are appropriate.

The Board also recognizes that telecommunications will allow citizens and school employees access to information sources that have not been prescreened by using Board approved standards. The Board therefore adopts the following standards of conduct for the use of computer networks and declares unethical, unacceptable or illegal behavior as just cause for taking disciplinary action, including, but not limited to, limiting or revoking network/internet access privileges and/or instituting legal action.

The Board provides access to computer network/computers for legal and ethical purposes only. Access is a privilege, not a right, and it is the policy of the Board to restrict *access to* any and all obscene and/or inappropriate materials. However, the Board recognizes that despite its best efforts to install network/computer system programming that blocks and screens offensive and inappropriate materials, it cannot guarantee that such materials will not be viewed. Therefore, it is incumbent upon all users of the system to be ultimately responsible for their use of the resource. Therefore, the Board retains the right to restrict or terminate a user or users' access to the computer network/computers at any time, for any reason. The Board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and insure its proper use.

STANDARDS FOR USE OF COMPUTER NETWORKS

- No user shall post personal contact information about themselves or other people. Personal contact information includes addresses, telephone numbers, work or school addresses and the like. No user shall agree to meet with any person who was met on-line. The Board takes no responsibility for such meetings and strongly- advises against them.

- All users shall promptly disclose to the person in charge of the computer lab on the day of an incident or other responsible staff member any message received that is inappropriate or makes the user uncomfortable.
- Users should have no expectation of privacy in the use of the Winfield computer/network system. The Board reserves the right to monitor every user's use of the system and such monitoring may lead to the discovery that a user violated this policy. Items contained in personal files are subject to review. The Board will fully and completely cooperate with any local, State or Federal agency that is investigating any illegal activities arising from the use of the Board's computer/network.

Any individual engaging in the following actions while using Winfield computer networks/computers shall be subject to discipline or legal action:

- A. Using the computer network(s)/computers for illegal, inappropriate or obscene purposes or in support of such activities. Illegal activities are defined as activities that violate federal, state, local laws and regulations. Inappropriate activities are defined as activities that violate the intended use of the computer/network. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles. Restrictions against inappropriate activities apply to public messages, private messages and materials posted on Web pages.

- B. Using the computer-networks/computers to violate copyrights, institutional or third party copyrights, license or other contracts.

- C. Using the computer-network(s) in a manner that:
 1. Intentionally disrupts network traffic or crashes the network;
 2. Degrades or disrupts equipment or system performance,
 3. Uses the computing resources of the school district for commercial purposes, financial gain or fraud;
 4. Steals data or other intellectual property;
 5. Gains or seeks unauthorized access to the files of others or vandalizes the data of another user;
 6. Gains or seeks unauthorized access to resources or entities;
 7. Forges electronic mail messages or uses an account owned by others
 8. Invades privacy of others;
 9. Posts anonymous messages;

10. Possesses any data which is a violation of this policy,
11. Engages in other activities that do not advance the educational purposes for which the Winfield computer network/computers are provided.
12. Engages in personal attacks, including prejudicial or discriminatory attacks, and/or
13. Knowingly posting private information, posting false or defamatory information about a person or organization.

- D. Gain or seek to gain unauthorized access to any other computer system beyond which is authorized within the system.
- E. Allow computer viruses to invade the network or any computer used at the school. Participate in chain letters or engage in "spamming" (sending an annoying or unnecessary message to a large number of people).
- F. Access information that is profane or obscene (pornography), that advocates illegal activities or that advocates violence or discrimination towards other people (hate literature).

CONSENT REQUIREMENT

No citizen or school employee shall be allowed to use the computer-network(s) and/or gain access to the Internet through the Winfield computers/network, unless they shall have first filed with the Superintendent or designee a signed consent form. The form of the consent form is attached hereto.

VIOLATIONS

Individuals violating this policy shall be subject to the consequences as indicated in the regulations as promulgated by the Superintendent and other appropriate discipline that includes but is not limited to:

1. Use of the network(s) only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. and/or Legal action and prosecution by the authorities.

Board Adoption Date: February 20, 2001

Board Approved: September 18, 2007

**Winfield Township Public Schools
Internet Permission Form**

Citizen and School Employee

As a user of the Winfield Township Public Schools Internet, I promise to follow the network rules. I understand that the use of on-line information retrieval and sharing is a privilege, not a right.

Name: _____ Address: _____ Date: _____
(Please Print)

I understand that access *to* electronic information, which includes the Internet, is designed for specific purposes. Policies and procedures are in place to restrict access to inappropriate material, but it is impossible for the Winfield Township Public School District to restrict access to all inappropriate material. Therefore, I will not hold Winfield Township Public Schools responsible for any inappropriate material acquired from this network. In addition, I understand that Winfield Township Public Schools does not assume responsibility for the accuracy or reliability of information obtained through access to remote sites. The use of on-line information retrieval and sharing is a privilege, not a right,

I have read this Internet Use Agreement and accept the limitations on access to the Internet.

User Name: _____ **Date:** _____

Signature _____ **Daytime#:** _____

Home Address _____ **Telephone#:** _____

Board Approved: September 18, 2007