

ACCESS TO TECHNOLOGY/ INTERNET USE  
TECHNOLOGY/ STUDENT SAFETY

The board shall work with the appropriate staff to 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. The Oxford Township Board of Education specifically disclaims any responsibility for the accuracy of information obtained through the Internet. Individuals who wish to have access to district technology and Internet agrees to abide by the provisions and conditions of the Internet Use form provisions. Any violations may result in disciplinary action, the revocation of the user's access privileges, and appropriate legal action. Any and all misuse of the information systems should be reported to the teacher, staff members or administration.

District Rights and Responsibilities

The computer system is the property of the Oxford Central School 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 ensure that teachers receive proper training in the use of the system; ensure that students are adequately supervised when using the system; maintain executed user agreements; and interpreting this acceptable use policy at the building level.

**Disclosure of Certain Student Information Via the Internet**

In accordance with N.J.A.C. 18A: 36-35, the board of education will assure that personally identifiable information shall not be disclosed on the district website without the prior written consent from the student's

parent or guardian. "Personally identifiable information" means students names, student photos, student e-mail accounts, student phone numbers, and locations and times of class trips.

6142.12R

### **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 (policy 6142.10)

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 districts networked or stand alone computers. An agreement and acknowledgement of the policy will be signed for all students by the student (grades 3-8) as well as a parent or guardian.. To deny a child access, parents/guardians must notify the chief school administrator 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 Students

Students in grades K-8 may have individual accounts at the request of teachers and with the consent of parents/guardians. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian.

### 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 as outlined in policy 4300.

### Supervision of Students

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

### **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 teachers 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 chief school administrator shall publish and disseminate guidelines on acceptable material for these web sites. The chief school administrator shall also ensure that district and school web sites do not disclose personally identifiable information about students 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 student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

## **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.

## **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.

This policy supersedes all previous policies and replaces policy 6061.6.

Date:

**First Adoption: March 21, 2002**

**Review Date: May 1, 2008**

**Revision and Adoption: June 26, 2008**

<b><u>Legal References:</u></b>	<u>N.J.S.A. 2A:38A-1 et seq.</u>	Computer System
	<u>N.J.S.A. 2C:20-25</u>	Computer Related Theft
	<u>N.J.S.A. 18A:7A-11</u>	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
	<u>N.J.S.A. 18A:36-35</u>	School Internet websites; disclosure of certain student information prohibited
	<u>N.J.A.C. 6A:10A-1.1 et seq</u>	<i>Improving Standards-Driven Instruction and Literacy and Increasing Efficiency in Abbott School Districts</i>
	<u>See particularly:</u>	
	<u>N.J.A.C. 6A:10A, Appendix A</u>	
	<u>N.J.A.C. 6A:30-1.1 et seq.</u>	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
	<u>N.J. v. T.L.O.</u> 469 U.S. 325 (1985)	
	<u>O'Connor v. Ortega</u> 480 U.S. 709 (1987)	
	<u>No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.</u>	

**Possible**

<b><u>Cross References:</u></b>	1111	District publications
	3514	Equipment
	<b>3543</b>	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)
	6142.10	Employee Use of Internet/ Technology
	6144	Controversial issues
	6145.3	Publications
	6161	Equipment, books and materials

**Key Words**

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