TELECOMMUNICATIONS / TECHNOLOGY

The Old Tappan Board of Education is committed to the development and establishment of a quality, equitable and cost-effective electronic telecommunications system, including Internet services. The system's sole purpose shall be for the advancement and promotion of learning and teaching. While there are many valuable uses of the Internet and the District's telecommunications system, there is the possibility of encountering offensive or inappropriate material on the Internet, despite the Old Tappan Board of Education's efforts to prohibit and guard against access to such material. However, the benefits of a student's use of the District's telecommunications system and the Internet far outweigh these potential detriments.

The District's system will be used to provide local, state-wide, 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. Beginning in the 2014/2015 school year, the District shall incorporate instruction on the responsible use of social media into the technology education curriculum for students in grades 6 through 8 as part of the implementation of the core curriculum standards.

It is the policy of the district to establish safe and effective methods for student and staff users of the district's technological resources and to:

A. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

B. Prevent unauthorized access and other unlawful online activity;

C. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

D. Comply with the Children's Internet Protection Act (CIPA).

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. In addition, the administration has the right to remove exchange or move any technological equipment at any time.

Staff members must be cognizant of and exercise the proper care of all technological equipment.

TECHNOLOGY/TELECOMMUNICATIONS (continued)

District Rights and Responsibilities (continued)
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 resources 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 Superintendent shall establish administrative regulations for the use of the District's system and assign a staff member as telecommunications systems manager. The regulations shall be consistent with District policy and pertinent state and federal law. These regulations must be reviewed at least annually to reflect changes in telecommunications.

If the District provides or loans students computers or other electronic equipment, the District shall include in its regulations, information on parental/guardian notification of the capabilities of such equipment as well as its statement that it will not violate the privacy rights of the student or individuals residing with the student.

This policy shall govern all use of the system. Failure to abide by District policy and administrative regulations governing use of the District's system may result in the suspension and/or revocation of system access as well as civil and/or criminal penalties. Student violations may result in discipline (see Policy 5131 Conduct/Discipline.) Staff violations may also result in discipline. Additionally, a student's parent(s) or legal guardian(s) shall be responsible for any damages which the student causes or any legal liability that results from the student's use of the District's telecommunications system and the Internet.

Parental Notification and Responsibility
The Superintendent shall ensure that parents/guardians are notified about the district network and the rules governing its use. No student will be permitted to use the District's telecommunications system unless and until the student and his/her parents (if the student is less than 18 years old) sign the District's Consent and Release Form which acknowledges that:

A. The student and his/her parent have read and understand this policy and the accompanying regulation;

B. The student will be held accountable for all of his/her network and Internet activities;

C. The student is expected to comply with the District's policy and regulation and all federal, state and local laws governing Internet use; and

D. The student and his/her parent shall indemnify and hold harmless the Old Tappan Board of Education, its members, agents, servants and employees from any and all liability relating to the student's use of the District's telecommunications system or the Internet.

Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Additionally, all teachers are required to discuss the technology policy and regulation with each of his/her classes and sign an acknowledgment that they have had such a discussion with his/her classes and the date(s) on which said discussions occurred.

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. The Board shall ensure the acquisition and installation of

TECHNOLOGY/TELECOMMUNICATIONS (continued)

World Wide Web (continued)
blocking/filtering software to deny access to certain areas of the Internet. An agreement shall be required. To deny a child access, parents/guardians must notify the Building Principal in writing.

COMPLIANCE WITH CIPA

A. Filters Blocking Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

B. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the school district online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

1. Unauthorized access, including so-called "hacking," and other unlawful activities; and

2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

C. Education, Supervision and Monitoring

It shall be the responsibility of all members of the school district staff to educate, supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Superintendent or his or her designee.

The Superintendent or his or her designee shall ensure that students and staff who use the school internet facilities receive appropriate training including the following:

1. The district established standards for the acceptable use of the internet;

2. Internet safety rules;

3. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;

4. Cyberbullying (board policy 5131.2 Harassment, Intimidation and Bullying) awareness and response.

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

TECHNOLOGY/TELECOMMUNICATIONS (continued)

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.

Classroom Email Accounts
Students in grades K-8 shall be granted email access through classroom accounts only. To deny a child access to a classroom account, parents/guardians must notify the Building Principal in writing.

Individual Email Accounts for District Employees
District employees shall be provided with an individual account and dial-up access to the system. An agreement shall not be required, but the rules and regulations will be discussed with all staff.

Supervision of Students
Student use of the Internet shall be supervised by qualified staff. Student use of teacher established blogs shall be regulated and supervised.

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 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" shall include but not be limited to student names, photos, addresses, email addresses, phone numbers, social security numbers, instant message addresses, and locations and times of class trips.

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 or discriminatory 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.

TECHNOLOGY/TELECOMMUNICATIONS (continued)

Prohibited Activities (continued)
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, but is not limited 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, discriminatory, or threatening language. Inadvertent access to such material should be reported immediately to the Building Principal.

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 if they detect a possible security problem. Users shall not access the system 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 email 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.

Intellectual Property and Plagiarism
Because certain works found on the Internet are protected by copyright, trademark, and other forms of intellectual property, employees will either request permission from the owner of the intellectual property rights prior to using any materials obtained on the Internet, or the employee will consult with the administration to determine whether the materials may be used without receiving permission based on certain exceptions to intellectual property rights as set forth in the relevant laws. Teachers will instruct students to adhere to the same guidelines.

TECHNOLOGY/TELECOMMUNICATIONS (continued)

Intellectual Property and Plagiarism (continued)
Users will be held personally liable for any of their own actions that violate another party's intellectual property rights. District practices on plagiarism will govern the use of materials accessed through the Internet. Teachers will instruct students as to the definition of plagiarism and the proper method to cite materials.

Policy Development
The District Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

Implementation
The Superintendent shall prepare regulations to implement this policy.

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-10 et seq.	New Jersey Quality Single Accountability Continuum for evaluating education
N.J.S.A. 18A:36-35	School internet websites; disclosure of certain student information prohibited
N.J.S.A.18A:36-39	Notification by school to certain persons using certain electronic devices; fine
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 CFR 54.503(d)	Competitive bidding; gift restrictions
47 U.S.C. 254(h)	Children's Internet Protection Act
NJ P.L.2013, c.44.	Anti Big Brother Act

State in re T..L.O 94 N.J. 331 (1983) reversed on other grounds N.J. v. T.L.O. 569 U.S. 325 (1985)

O'Connor v. Ortega 480 U.S. 709 (1987)

COPPA

Anti-Bullying Rights Act

O'Connor v. Ortega 480 U.S. 709 (1987)

P.L.2013, c.257 Social Media Use

No Child Left Behind Act of 2001 Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

Cross References:

*1111	District publications
*3514	Equipment
3543	Office services
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	Student safety

TECHNOLOGY/TELECOMMUNICATIONS (continued)

Cross References: (continued)

5145.2	Freedom of speech/expression (students)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

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

Key Words

Acceptable Use, Blocking/Filtering Software, Email, Internet, Technology, Web Site, World Wide Web, Anti-Big Brother Act, Social Media Use

Approved: November 23, 1998
Revised: June 9, 2008, September 10, 2012, May 13, 2013, March 10, 2014, May 23, 2016, October 24, 2016