

POLICY

**BOARD OF EDUCATION
WASHINGTON TOWNSHIP
PROGRAM**

2361/page 1 of 4

**Student Acceptable Use of
Computer Network/ Computers
and Resources**

2361 STUDENT ACCEPTABLE USE OF COMPUTER
NETWORK/COMPUTERS AND RESOURCES

I. Definitions:

“Computer network” refers to the District’s wired and wireless Wide Area Network (WAN) which provides both local network and external internet access.

“Computer/Technology” includes, but not limited to, desktop computers, laptops, tablets, smart phones, MP3 Players, or any wired or wireless communication device.

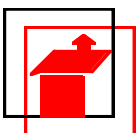
“District Technology” is that which is owned or provided by the Washington Township School District.

“Personal Technology” is non-district owned technology.

The Board of Education recognizes as new technologies shift the manner in which information is accessed, communicated, and transferred; these changes alter the practice and means of teaching and learning today. Access to technology will allow pupils to explore databases, libraries, Internet sites, and forums/message boards while exchanging information with individuals throughout the world. The Board supports access by pupils to these resources but reserves the right to limit in school use to materials appropriate for educational purposes. The Board directs the Superintendent to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes and to infuse these resources into the curriculum.

The Board also recognizes technology allows pupils access to information sources that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following standards of conduct for the use of technology and declares unethical, or illegal behavior as just cause for taking disciplinary action, limiting or revoking network/computer access privileges and/or instituting legal action.

The Board provides access to the computer network/computers primarily for educational purposes. The Board retains the right to restrict or terminate pupil access to the computer network/ computers at any time, for any reason. School district personnel will monitor networks and online activity, to maintain the integrity of the networks, ensure their proper use, and ensure compliance with Federal and State laws that regulate Internet safety.



POLICY

**BOARD OF EDUCATION
WASHINGTON TOWNSHIP
PROGRAM**

2361/page 2 of 4

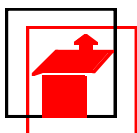
**Student Acceptable Use of
Computer Network/ Computers
and Resources**

Standards for Use of Computer Networks

Any individual engaging the following actions when using 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 those that violate the intended use of the network. The use of the network is defined as primarily for educational purposes. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication devices.
- B. Using the computer network/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts. (The Copyright Act U.S.C § 106)
- C. Using the computer network in a manner that:
 - 1. Intentionally disrupts network traffic or crashes the network;
 - 2. Degrades or disrupts equipment or system performance;
 - 3. Uses the technology 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 person;
 - 6. Gains or seeks unauthorized access to resources or entities;
 - 7. Uses any technology to circumvent the district's web filter and/or firewalls in order to gain access to otherwise prohibited materials;
 - 8. Forges electronic messages or uses an account owned by others;
 - 9. Invades privacy of others;
 - 10. Posts harassing/threatening anonymous messages;
 - 11. Possesses any data which is a violation of this Policy; and/or
 - 12. Engages in other activities that do not advance the educational purposes for which computer network/computers are provided.

Internet Safety/Protection



POLICY

**BOARD OF EDUCATION
WASHINGTON TOWNSHIP
PROGRAM**

2361/page 3 of 4

**Student Acceptable Use of
Computer Network/ Computers
and Resources**

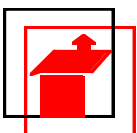
As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act (CIPA), the Neighborhood Children's Internet Protection Act (NCIPA), and has installed content filters and firewalls on all computers and devices in the school district. The content filters must make a reasonable attempt to block and/or filter material or visual depictions that are obscene as defined in section 1460 of Title 18, United States Code; child pornography, as defined in section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

This Policy also establishes Internet safety policies and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identifiable information regarding minors without parental consent; and measures designed to restrict minors' access to materials harmful to minors.

Notwithstanding blocking and/or filtering the material and visual depictions prohibited in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure instruction is provided to every pupil regarding appropriate online behavior, including pupils interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.



POLICY

**BOARD OF EDUCATION
WASHINGTON TOWNSHIP
PROGRAM**

2361/page 4 of 4

Student Acceptable Use of
Computer Network/ Computers
and Resources

Consent Requirement

No pupil shall be allowed to use the school districts' computer network/computers and the Internet unless he/she has filed with the building principal, a consent form signed by the pupil and his/her parent(s) or legal guardian(s).

Violations

Individuals violating this Policy shall be subject to the consequences as indicated in Regulation 2361 and other appropriate disciplinary action, which include but are not limited to:

1. Use of the network only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of technology privileges;
5. Revocation of technology privileges;
6. School disciplinary action (e.g., detentions, Saturday School, suspension, etc.);
7. Expulsion from school;
8. Withdrawal from course with loss of credit (Middle School/High School); and/or
9. Legal action and prosecution by the authorities.

N.J.S.A. 2A:38A-3

Federal Communications Commission: Children's Internet Protection Act.

Federal Communications Commission: Neighborhood Children's Internet Protection Act

Adopted: 25 August 1998

Revised & Approved: 23 October 2001 [Policy Alert 157]

Revised & Approved: 29 June 2004

Revised & Approved: 25 August 2015 [Policy Alert 197]

