

2361 ACCEPTABLE USE OF COMPUTER NETWORKS/
COMPUTERS AND RESOURCES

The Board of Trustees recognizes as new technologies shift the manner in which information is accessed, communicated, and transferred; these changes will alter the nature of teaching and learning. Access to technology will allow students to explore databases, libraries, Internet sites, and bulletin boards while exchanging information with individuals throughout the world. The Board supports access by students to these information sources but reserves the right to limit in-school use to materials appropriate for educational purposes. The Board directs the Directors to effect training of teaching staff members in skills appropriate to analyzing and evaluating such resources as to appropriateness for educational purposes.

The Board also recognizes technology allows students 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 computer networks and declares unethical, unacceptable, or illegal behavior as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The Board provides access to computer networks/computers for educational purposes only. The Board retains the right to restrict or terminate student access to computer networks/computers at any time, for any reason. School 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.

Standards for Use of Computer Networks

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

- A. Using the computer networks/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 networks. Obscene activities shall be defined as a violation of generally accepted social standards for use of publicly owned and operated communication vehicles.
- B. Using the computer networks/computers to violate copyrights, institutional or third party copyrights, license agreements or other contracts.



POLICY

WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES

PROGRAM
2361/page 2 of 4
Acceptable Use of Computer Networks/
Computers and Resources

- C. Using the computer networks 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 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. 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; and/or
 11. Engages in other activities that do not advance the educational purpose for which computer networks/computers are provided.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school, including computers in media centers/libraries. The technology protection must block and/or filter material and 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 material or 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.



POLICY

WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES

PROGRAM
2361/page 3 of 4
Acceptable Use of Computer Networks/
Computers and Resources

This Policy also establishes Internet safety policy and procedures in the school as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; 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 identification information regarding minors; 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 Directors or their designee will develop and ensure education is provided to every student regarding appropriate online behavior, including students interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The school will certify on an annual basis, that the school, including media centers/libraries, is in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school enforces the requirements of these Acts and this Policy.

Consent Requirement

No student shall be allowed to use the school's computer networks/computers and the Internet unless they have filed a consent form signed by the student and his/her parents.

Violations

Individuals violating this Policy shall be subject to the consequences as indicated in Regulation 2361 and other appropriate discipline, which includes 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 computer privileges;



POLICY

**WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES**

PROGRAM
2361/page 4 of 4
Acceptable Use of Computer Networks/
Computers and Resources

5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. 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: 2 November 2018



REGULATION

WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES

PROGRAM

R 2361/page 1 of 8

Acceptable Use of Computer Networks/
Computers and Resources

R 2361 ACCEPTABLE USE OF COMPUTER NETWORKS/
COMPUTERS AND RESOURCES

The school provides computer equipment, computer services, and Internet access to its students and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources.

For the purpose of this Policy and Regulation, "computer networks/computers" includes, but is not limited to, the school's computer networks, computer servers, computers, other computer hardware and software, Internet equipment and access, and any other computer related equipment.

For the purpose of this Policy and Regulation, "school personnel" shall be the person(s) designated by the Directors to oversee and coordinate the school's computer networks/computer systems. School personnel will monitor networks and online activity, in any form necessary, to maintain the integrity of the networks, ensure proper use, and to be in compliance with Federal and State laws that regulate Internet safety.

Due to the complex association between government agencies and computer networks/computers and the requirements of Federal and State laws, the end user of the school's computer networks/computers must adhere to strict regulations. Regulations are provided to assure staff, community, students, and parents of students are aware of their responsibilities. The school may modify these regulations at any time. The signatures of the student and his/her parents on a school-approved Consent and Waiver Agreement are legally binding and indicate the parties have read the terms and conditions carefully, understand their significance, and agree to abide by the rules and regulations established under Policy and Regulation 2361.

Students are responsible for acceptable and appropriate behavior and conduct on school computer networks/computers. Communications on the computer networks/computers are often public in nature and policies and regulations governing appropriate behavior and communications apply. The school's networks, Internet access, and computers are provided for students to conduct research, complete school assignments, and communicate with others. Access to computer networks/computers is given to students who agree to act in a considerate, appropriate, and responsible manner. Parent permission is required for a student to access the school's computer networks/computers. Access entails responsibility and individual users of the school computer networks/computers are responsible for their behavior and communications over the computer networks/computers. It is presumed users will comply with school standards and will honor the agreements they have signed and the permission they have been granted. Beyond the clarification of such standards, the school is not responsible for the actions of individuals utilizing the computer networks/computers who violate the policies and regulations of the Board.



REGULATION

WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES

PROGRAM

R 2361/page 2 of 8

Acceptable Use of Computer Networks/
Computers and Resources

Computer networks/computer storage areas shall be treated in the same manner as other school storage facilities. School personnel may review files and communications to maintain system integrity, confirm users are using the system responsibly, and ensure compliance with Federal and State laws that regulate Internet safety. Therefore, no person should expect files stored on school servers will be private or confidential.

The following prohibited behavior and/or conduct using the school's networks/computers, includes but is not limited to, the following:

1. Sending or displaying offensive messages or pictures;
2. Using obscene language and/or accessing material or visual depictions that are obscene as defined in section 1460 of Title 18, United States Code;
3. Using or accessing material or visual depictions that are child pornography, as defined in section 2256 of Title 18, United States Code;
4. Using or accessing material or visual depictions that are harmful to minors including any pictures, images, graphic image files or other material or visual depictions that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
5. Depicting, describing, or representing 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;
6. Cyberbullying;
7. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;
8. Harassing, insulting, or attacking others;
9. Damaging computers, computer systems, or computer networks/computers;
10. Violating copyright laws;
11. Using another's password;
12. Trespassing in another's folders, work or files;



REGULATION

PROGRAM
R 2361/page 3 of 8
Acceptable Use of Computer Networks/
Computers and Resources

13. Intentionally wasting limited resources;
14. Employing the computer networks/computers for commercial purposes; and/or
15. Engaging in other activities that do not advance the educational purposes for which computer networks/computers are provided.

INTERNET SAFETY

Compliance with Children's Internet Protection Act

As a condition for receipt of certain Federal funding, the school has technology protection measures for all computers in the school, including computers in media centers/libraries, that block and/or filter material or visual depictions that are obscene, child pornography and harmful to minors as defined in 2, 3, 4, 5, 6, and 7 above and in the Children's Internet Protection Act. The school will certify the school, including media centers/libraries are in compliance with the Children's Internet Protection Act and the school complies with and enforces Policy and Regulation 2361.

Compliance with Neighborhood Children's Internet Protection Act

Policy 2361 and this Regulation establish an Internet safety protection policy and procedures to address:

1. Access by minors to inappropriate matter on the Internet and World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including "hacking" and other unlawful activities by minors online;
4. Cyberbullying;
5. Inappropriate online behavior, including inappropriate interaction with other individuals on social networking sites and in chat rooms;
6. Unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and
7. Measures designed to restrict minors' access to materials harmful to minors.

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



REGULATION

WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES

PROGRAM

R 2361/page 4 of 8

Acceptable Use of Computer Networks/
Computers and Resources

Information Content and Uses of the System

Students may not publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane, or sexually offensive to a reasonable person, or which, without the approval of the Directors or designated school personnel, contains any advertising or any solicitation to use goods or services. A student cannot use the facilities and capabilities of the system to conduct any business or solicit the performance of any activity which is prohibited by law.

Because the school provides, through connection to the Internet, access to other computer systems around the world, students and their parents should be advised the Board and school personnel have no control over content. While most of the content available on the Internet is not offensive and much of it is a valuable educational resource, some objectionable material exists. Even though the Board provides students access to Internet resources through the school's computer networks/computers with installed appropriate technology protection measures, parents and students must be advised potential dangers remain and offensive material may be accessed notwithstanding the technology protection measures taken by the school.

Students and their parents are advised some systems and Internet sites may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material. The Board and school personnel do not condone the use of such materials and do not permit usage of such materials in the school environment. Parents having Internet access available to their children at home should be aware of the existence of such materials and monitor their child's access to the school system at home. Students knowingly bringing materials prohibited by Policy and Regulation 2361 into the school environment will be disciplined in accordance with Board policies and regulations and such activities may result in termination of such students' accounts or access on the school's computer networks and their independent use of computers.

On-line Conduct

Any action by a student or other user of the school's computer networks/computers that is determined by school personnel to constitute an inappropriate use of the school's computer networks/computers or to improperly restrict or inhibit other persons from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending person's access and other consequences in compliance with Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal or offensive material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, State or Federal law is also prohibited and is a breach of the Consent and Waiver Agreement.



REGULATION

Students and their parents specifically agree to indemnify the school and school personnel for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the student.

Computer networks/computer resources are to be used by the student for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network

Software libraries on or through the school's networks are provided to students as an educational resource. No student may install, upload, or download software without the expressed consent of appropriate school personnel. Any software having the purpose of damaging another person's accounts or information on the school computer networks/computers (e.g., computer viruses) is specifically prohibited. School personnel reserve the right to refuse posting of files and to remove files. School personnel further reserve the right to immediately limit usage or terminate the student's access or take other action consistent with the Board's policies and regulations of a student who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the computer networks/computers without authorization. Students may download copyrighted material for their own use in accordance with Policy and Regulation 2531 - Use of Copyrighted Materials. A student may only redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author or authorized source.

Public Posting Areas (Message Boards, Blogs, Etc.)

Messages are posted from systems connected to the Internet around the world and school personnel have no control of the content of messages posted from these other systems. To best utilize system resources, school personnel will determine message boards, blogs, etc. that are most applicable to the educational needs of the school and will permit access to these sites through the school computer networks. School personnel may remove messages that are deemed to be unacceptable or in violation of Board policies and regulations. School personnel further reserve the right to immediately terminate the access of a student who misuses these public posting areas.

Real-time, Interactive, Communication Areas

School personnel reserve the right to monitor and immediately limit the use of the computer networks/computers or terminate the access of a student who misuses real-time conference features (talk/chat/Internet relay chat).



REGULATION

PROGRAM
R 2361/page 6 of 8
Acceptable Use of Computer Networks/
Computers and Resources

Electronic Mail

Electronic mail ("email") is an electronic message sent by or to a person in correspondence with another person having Internet mail access. The school may or may not establish student email accounts. In the event the school provides email accounts, all messages sent and received on the school computer networks/computers must have an educational purpose and are subject to review. Messages received by a school-provided email account are retained on the system until deleted by the student or for a period of time determined by the school. A canceled account will not retain its emails. Students are expected to remove old messages within fifteen days or school personnel may remove such messages. School personnel may inspect the contents of emails sent by a student to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the policy, regulation, or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, State, or Federal officials in any investigation concerning or relating to any email transmitted or any other information on the school computer networks/computers.

Disk Usage

The school reserves the right to establish maximum storage space a student receives on the school's system. A student who exceeds his/her quota of storage space will be advised to delete files to return to compliance with the predetermined amount of storage space. A student who remains in noncompliance of the storage space allotment after seven school days of notification may have their files removed from the school's system.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a student identifies a security problem on the computer networks/computers, the student must notify the appropriate school staff member. The student should not inform other individuals of a security problem. Passwords provided to students by the school for access to the school's computer networks/computers or developed by the student for access to an Internet site should not be easily guessable by others or shared with other students. Attempts to log in to the system using either another student's or person's account may result in termination of the account or access. A student should immediately notify the Principal or designee if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any student identified as a security risk will have limitations placed on usage of the computer networks/computers or may be terminated as a user and be subject to other disciplinary action.



REGULATION

Vandalism

Vandalism to any school owned computer networks/computers may result in cancellation of system privileges and other disciplinary measures in compliance with the school's discipline code. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other computer networks/computers that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer networks/computers should be used judiciously. Unauthorized printing for other than educational purposes is prohibited.

Internet Sites and the World Wide Web

Designated school personnel may establish an Internet site(s) on the World Wide Web or other Internet locations. Such sites shall be administered and supervised by designated school personnel who shall ensure the content of the site complies with Federal, State, and local laws and regulations as well as Board policies and regulations.

Violations

Violations of the Acceptable Use of Computer Networks/Computers and Resources Policy and Regulation may result in a loss of access as well as other disciplinary or legal action. Disciplinary action shall be taken as indicated in Policy and/or Regulation, 2361 - Acceptable Use of Computer Networks/Computers and Resources, 5600 - Student Discipline/Code of Conduct, 5610 - Suspension and 5620 - Expulsion as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this Policy shall be determined by the Principal or designee. The Directors or their designee and the Board shall determine when school expulsion and/or legal action or actions by the authorities is the appropriate course of action.

Individuals violating this Policy shall be subject to the consequences as indicated in Board Policy and Regulation 2361 and other appropriate discipline, which includes but is not limited to:

1. Use of computer networks/computers only under direct supervision;



REGULATION

**WINDSOR LEARNING CENTER
WINDSOR SCHOOL
BOARD OF TRUSTEES**

PROGRAM
R 2361/page 8 of 8
Acceptable Use of Computer Networks/
Computers and Resources

2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from school;
7. Expulsion from school; and/or
8. Legal action and prosecution by the authorities.

Issued: 2 November 2018

