**ORADELL PUBLIC SCHOOL DISTRICT**
**Oradell, New Jersey**

**Policy**

**FILE CODE: 6142.10**
**_____ Monitored**
**_X_ Mandated**
**_X_ Other Reasons**

# INTERNET SAFETY AND TECHNOLOGY

The Oradell Board of Education 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 New Jersey Student Learning Standards.

To support the district's commitment to providing avenues of access to the universe of information available, the system of electronic communication shall include access to the Internet for students and staff. To remain eligible as users, students and adults must restrict their activities to endeavors that are in support of and consistent with the educational objectives of the school district. The district expects that faculty will apply the thoughtful use of all available technology resources to the learning environment, making such an integral part of curriculum delivery.

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).

The district shall ensure equal and bias-free access for all students to computers, computer classes, career and technical education programs, and technologically-advanced instructional assistance, regardless of race, creed, color, national origin, ancestry, age, marital status, affectional/sexual orientation, gender, religion, disability, English proficiency, immigration status, housing status or socioeconomic status.

## COMPLIANCE WITH CIPA

### 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.

### 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:

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

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

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 chief school administrator or his or her designee.

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

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

B. Internet safety rules;

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

D. Cyberbullying (board policy 5131.1 Harassment, Intimidation and Bullying) awareness and response.

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

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.

## 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 principal shall coordinate the district system in his/her building by approving all activities for that 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 network. Sanctions for student misuse of the network shall be as follows, based on the severity of the situation:

A. Suspension of computer/network privileges;

B. Revocation of computer/network privileges;

C. Suspension from school;

D. Expulsion from school; and/or

E. Legal action and prosecution by the authorities

Employee misuse may result in appropriate discipline/legal action in accord with 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. To the extent practical, technology protection measures (or "Internet Filters") shall be used to block or filter access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act (CIPA), 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 for bona fide research or other lawful purposes.

Internet

All students and employees of the board shall have access to the Web through the district's networked or stand alone computers. An agreement may be required. A parent/student form acknowledging receipt and review of this policy shall be required in grades 2 through 6. To deny a child access, parents/ guardians must notify the building principal in writing. The board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual e-mail account and access to the system. An agreement shall not be required. The account will be publicized to facilitate parent-faculty communications.

Supervision of Students

Student use of the Internet shall be supervised by qualified, contracted staff. The use of search engines independently by students shall be limited to those highlighted on the Oradell Public School Web Site and in

INTERNET SAFETY TECHNOLOGY (continued)

the Oradell Network User's Guide. Students are prohibited from using other search engines (i.e. Google) unless under the supervision of the classroom teacher.

Use of Computer Network/Computers by the Oradell Education Association

The Oradell Education Association shall be granted permission to use the computer network/computers for legitimate Association business only. It is expressly understood that the computer network/computers shall not be used, under any circumstances, by any staff member to communicate any information concerning job actions, boycotts, work stoppages, strikes, sanctions, or any other concerted activities against either the Board or the district that could be considered to be obstructive to the educational program during any labor negotiations.

District Website

The board authorizes the chief school administrator to establish and maintain a district website. 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 chief school administrator shall develop guidelines for the establishment and maintenance of the district website and web pages. 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. In addition, teachers shall not post such personal information about their students. 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 containing text with personal information.

Prohibited Activities

To the extent practical, steps shall be taken to promote the safety and security of users of the Library's 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:

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

INTERNET SAFETY TECHNOLOGY (continued)

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

In compliance with the Children's Internet Protection Act, users shall not commit acts of harassment, intimidation, or bullying using the computer or its network and are reminded that any act of harassment, intimidation, or bullying is prohibited.

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.

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.

School Furnished Electronic Devices

The district may furnish students electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices. When a student is furnished with an electronic device the district shall provide the student with written or electronic notification that the electronic device may record or collect information on the student's activity or the student's use of the device if the electronic device is equipped with a camera, global positioning system, or other feature capable of recording or collecting information on the student's activity or use of the device. The notification shall also include a statement that the district shall not use any of the capabilities in a manner that would violate the privacy rights of the student or any individual residing with the student. The parent or guardian of the student furnished an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgement as long as the student retains the use of the electronic device.

Failure to provide the required notification shall be subject to a fine of $250 per student, per incident. If imposed, the fine shall be remitted to the Department of Education, and shall be deposited in a fund that shall be used to provide laptop or other portable computer equipment to at-risk students.

Faculty and Student Rights

A. Free Speech

The right to free speech for staff and students applies to personal communication on the Internet. However, communication on the Oradell Public School District Network (OPSDN) is considered a limited forum similar to a school newspaper or similar student publication. Therefore, the district may restrict your speech for valid educational reasons. The district will not restrict your speech on the basis of a disagreement with the opinions you are expressing.

B. Search and Seizure

1. No user can expect privacy in the contents of email files on the district system. The email system and all computer systems are the property of the Oradell Public School. Staff and students do not have personal property rights in any matter created, received or sent from the email or other systems on the OPSDN. All users are hereby put on notice that any and all email files are subject to review and inspection by the Oradell Public School faculty and administration. All emails sent or received via the Oradell Public School District Network are archived for three (3) years per governmental regulations;
2. Routine maintenance and monitoring of the OPSDN may lead to discovery of behavior in violation of board policy, the Oradell Public School disciplinary code, or the law;
3. Students' parents/guardians have the right, at any time, to view those files containing the work products of their children.

C. Due Process

1. The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the OPSDN;
2. In the event there is a claim that you have violated this policy or any of the Oradell Public School disciplinary procedures in your use of the OPSDN, The staff member or student involved will be provided with a written notice of the suspected violation and an opportunity to present an explanation to an administrator (or will be provided with notice and opportunity to be heard in the manner set forth in the disciplinary procedures);
3. If the violation also involves a violation of other provisions of the Oradell Public School policy, it will be handled in a manner described within the district's policy and procedures manual. Additional restrictions may be placed on internet use if a violation is verified.

Implementation

INTERNET SAFETY TECHNOLOGY (continued)

The chief school administrator shall disseminate this policy to all staff members. Students and their parents will be referred to the district's Parent-Student Handbook and website regarding acceptable use of the Internet.

| | |
|---|---|
| Adopted: | December 9, 2009 |
| Revised: | October 17, 2012, September 12, 2013, May 24, 2016 |
| NJSBA Review/Update: | August 2018, January 2019 |
| Readopted: | December 12, 2018, December 11, 2019 |
| Reviewed: | |

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Internet Safety, Technology, Website, World Wide Web, CIPA

**Legal References**: N.J.S.A. 2A:38A-1 et seq. Actions for computer related offenses
N.J.S.A. 2C:20-25 Computer criminal activity; degree of crime; sentencing
N.J.S.A. 18A:7A-10 NJQSAC
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:30-1.1et 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

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

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

Every Student Succeeds Act of 2015, Pub. L. 114-95, 20 U.S.C.A. 6301 et seq.

**Possible Cross References:**

| | |
|---|---|
| *1111 | District publications |
| *3514 | Equipment |
| *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 |
| *5131.1 | Harassment, intimidation and bullying |
| *5131.5 | Vandalism/violence |
| *5142 | Student safety |
| *6144 | Controversial issues |
| *6145.3 | Publications |

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