INTERNET SAFETY AND TECHNOLOGY/ ACCEPTABLE USE OF THE COMPUTER NETWORK, COMPUTERS AND RESOURCES

The board 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 the New Jersey Student Learning 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) and the Children's Online Privacy Protection Act (COPPA).

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 chief school administrator or his or her designee shall approve all activities in the school; 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 interpret this acceptable use policy.

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 Board policy 5131 (Conduct and Discipline).

Employee misuse may result in appropriate discipline in accord with the collective bargaining agreement and 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.

World Wide Web

All students and employees of the board shall have access to the Internet through the district's networked or stand alone computers. An agreement shall be required. To deny a child access, parents/guardians must notify the building principal in writing.

COMPLIANCE WITH CIPA/ COPPA

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 (CIPA) and the Children's Online Privacy Protection Act (COPPA), 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 CIPA/ COPPA, 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, CIPA and COPPA. 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.

Monitoring and Privacy

Users have no right to privacy while using the Oxford Central School Internet Systems or an Internet provider outside the school. The Oxford Central School monitors users' online activities and reserves the right to access, review, copy, store, or delete any electronic communications or files. This includes any items stored on district-provided devices, such as files, e-mails, cookies, and Internet history.

The school district reserves the right to disclose any electronic activity, including electronic communications, to law enforcement officials or third parties, as appropriate and consistent with applicable law. The district will fully cooperate with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the Oxford Central School Internet Systems.

Prohibited Uses of the Oxford Central School Internet Systems

Users may not engage in any of the activities prohibited by this policy when using or accessing the Oxford Central School Internet Systems.

If a user is uncertain whether behavior is prohibited, he or she should contact a teacher, or appropriate personnel. The district reserves the right to take immediate action regarding activities that (1) create security and/or safety issues for the district, students, employees, schools, network or computer resources, or (2) expend district resources on content the district determines lacks legitimate educational or district content or purpose, or (3) the district determines are inappropriate.

Below is a **non-exhaustive** list of examples of prohibited behavior:

1. Causing harm to others, damage to their property or district property, such as:

- Using, posting or distributing profane, lewd, vulgar, threatening, or abusive language in e-mail messages, material posted on district web pages, or professional social media sites;
- Accessing, using, posting, or distributing information or materials that are pornographic or otherwise obscene, advocate illegal or dangerous acts, or advocate violence or discrimination. If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school or central division office;
- Accessing, posting or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statements about others;
- Sending, posting, or otherwise distributing chain letters or engaging in spamming;
- Damaging computer equipment, files, data or the district's Internet System in any way, including spreading computer viruses, vandalizing data, software or equipment, damaging or disabling others' electronic property, or engaging in conduct that could interfere or cause a danger of disruption to the district's educational or business environment;
- Using the Oxford Central School's Internet System in a manner that interferes with the education of the user or others or the job duties of the user or others;
- Downloading, posting, reproducing or distributing music, photographs, video or other works in violation of applicable copyright laws. Any music, photographs and/or video should only be downloaded for district, and not personal purposes. If a work specifies how that work may be used, the user should follow the expressed requirements. If users are unsure whether or not they can use a work, they should request permission from the copyright or trademark owner; or
- Engaging in plagiarism. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

2. Gaining or attempting to gain unauthorized access to the district's Internet Systems, or to any third party's computer system, such as:

- Malicious tampering, phishing or hacking activities;
- Intentionally seeking information about passwords belonging to other users;
- Disclosing a user's password to the district's Internet Systems to other individuals. However, students may share their district password with their parents.
- Modifying passwords belonging to other users;
- Attempting to log in through another person's account;
- Attempting to gain access to material that is blocked or filtered by the district;
- Accessing, copying, or modifying another user's files without authorization;
- Disguising a user's identity;
- Using the password or identifier of an account that does not belong to the user; or
- Engaging in uses that jeopardize access into others' accounts or other computer networks.

3. Using the Oxford Central School's Internet Systems for commercial purposes, such as:

- For personal financial gain;
- Conducting for-profit business activities or personal advertising;
- Engaging in fundraising; or
- Using the district's Internet Systems on behalf of any elected official, candidate, candidates, slate of candidates or a political organization or committee.

4. Engaging in criminal or other unlawful activities.

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.

Individual E-mail Accounts for District Employees and Students

District employees shall be provided with email access. Access to the system will be provided for staff members who have signed the acceptable use policy agreement. Email will be monitored and archived for three years. Employee email is discoverable and will be released if subpoenaed within the archival period set forth in this policy. Students will be provided with Google email accounts for access to the Google Applications for Education.

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.

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.

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 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. After the second marking period, all passwords will be changed.

System Limits

Employees 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 may prepare regulations to implement this policy.

Date:
First Adoption: March 21, 2002
Review Date: May 1, 2008
Revision and Adoption: June 26, 2008
Review Date: July 20, 2011 – No Changes
Review Date: May 16, 2012
Revision and First Reading: June 28, 2012
Second Reading and Adoption: July 26, 2012
Review Date: August 3, 2016
Revision and Adoption: August 18, 2016
Review Date: June 22, 2017
Revision and Adoption: July 20, 2017

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 school performance
N.J.S.A. 18A:36-35	School Internet websites; disclosure of certain student information prohibited
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 U.S.C. 254(h)	Children's Internet Protection Act

15 U.S.C. 6501-6505, Children's Online Privacy Protection Act
16 CFR Part 312

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)

20 U.S.C. 6301 et seq Every Student Succeeds Act (Formerly NCLB)

Possible Cross References:

1111	District publications
3514	Equipment
3543	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
5131.1	Harassment, Intimidation, Bullying
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