TOWNSHIP OF UNION BOARD OF EDUCATION **FILE CODE: 6142.10**
Union, New Jersey **_____ Monitored**
__X__ Mandated
Policy **__X__ Other Reasons**

TECHNOLOGY

The Township of Union 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 the Core Curriculum Content Standards.

The use of technology within the district is intended for school-related work and is designed to facilitate learning. It is the policy of the district to establish safe and effective methods for staff and student users of the district's technology resources, and to: (a) prevent user access to and the transmission of inappropriate material via any form of electronic communication; (b) prevent unauthorized access and online activity; and (c) comply with the Children's Internet Protection Act (CIPA).

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.

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.

The district's design and development of technological resources are devoted to the pursuit of academic growth, research, career readiness and professional development activities consistent with the educational objectives of the district. The district expects all users to agree to this policy as a condition of receiving Internet access. Usage is a privilege not a right and can be revoked at any time.

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 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 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.

TECHNOLOGY (continued)

Each 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 system. Sanctions for student misuse of the system shall be included in the disciplinary code for students, as set out in regulations for policy 5131 Conduct/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 Web 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.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual account and access to the system. An agreement shall be required.

1. Full-time district employees will be provided an e-mail account and access to the system.
2. The district computer system and the contents thereof are the property of the district.
3. E-mail is provided for the purpose of exchanging information consistent with the mission of the district. E-mail messaging on the district's computer system is intended for official business.
4. The information on the network belongs to the district. The district reserves the right to monitor messaging on the system to the extent permissible by law.
5. All correspondence protocols observed in the flow of paper communication must be similarly adhered to in e-mail transactions. Appropriate approvals of correspondence must take place before e-mail is sent to recipients.
6. Non-essential announcements such as office greetings and general notifications (without appropriate approval) should not be posted on District E-mail.
7. Users must not post chain letters or engage in "spamming". Spamming is the sending of an annoying and unnecessary message to a large number of people.
8. While engaged in activities on the District computer network, users are prohibited from transmitting E-mail to others that includes material that is vulgar, rude, obscene, pornographic, inflammatory, threatening, harassing, disrespectful or which uses sexually explicit language.
9. Users should not expect their E-mail communications to be private, and should not use district e-mail for confidential matters that are not intended for public disclosure.
10. Unauthorized attempts to read, delete, copy or modify e-mail of other users is prohibited.
11. All users must adhere to the same standards for communicating online that are expected in the classroom and that are consistent with district policies, regulations and procedures.

Supervision of Students

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

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.

TECHNOLOGY (continued)

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" refers to student names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

Parental Notification and Responsibility

The superintendent 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

It is the responsibility of the school staff to educate and provide ongoing guidance for students on personal safety practices, appropriate on-line behavior, cyber-bullying awareness and response, and effective techniques for identifying and evaluating information and its sources. School staff shall be required to supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy.

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 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 act or action that violates local, state or federal laws.

Users may not use the computer network to access, send post, transmit, distribute, publish, display, download or store false or defamatory information about a person, organization or group that is abusive, pornographic, obscene or otherwise offensive, or statements that advocate hate, violence or harassment and discrimination toward others or to harass another person or engage in personal attacks.

Users may not use the network for private or commercial business use, political or religious purposes.

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 (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 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.

Attempts to log on as any other user will result in cancellation of user privileges. Users who have been identified as a security risk, or having a history of problems with other computer systems will be denied access to the Internet.

Under no circumstances should users give passwords to other individuals or sign other users onto their account.

Vandalism will result in cancellation of privileges and possible disciplinary or legal action. Vandalism is defined as any malicious or intentional attempt to harm or destroy data of another user, the destruction of computer equipment or other property, the theft or defacing of computer equipment. This also includes the intentional uploading or creation of computer viruses when using the Internet.

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.

Users must take reasonable precautions to prevent virus infections on the district's equipment.

The downloading of any software or files without the approval of the Director of IT is strictly prohibited. Software is defined as but not limited to programs, games, browsers and sound files, which can be downloaded from the Internet.

The illegal use of copyrighted software or files is prohibited. Copyright infringement occurs when you use and/or reproduce a work that is protected by a copyright.

The accessing of non-educational content programs, games, chat rooms and recreational videos and music is strictly prohibited.

The district does not relinquish control over materials on the computer system or contained in files stored on the system.

The district reserves the right to suspend or terminate the computer access of users who have violated the AUP, and to delete or remove files found to be in violation of the AUP.

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.

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources.

Implementation

The superintendent shall prepare regulations to implement this policy.

Adopted:	June 1999; August 16, 2001
NJSBA Review/Update:	April 2012
Readopted:	April 29, 2014

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web, **Internet safety, cyber-bullying, social networking.**

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

15 U.S.C. § 6501-6506 Children's Online Privacy Protection Act

15 U.S.C. § 6551-6555 Promoting a Safe Internet for Children 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)

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

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
*5131.5	Vandalism/violence
*5142	Student safety
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.