MORRIS COUNTY VOCATIONAL SCHOOL
Denville, New Jersey

FILE CODE: 6142.10
_X_ Monitored
_X_ Mandated
_X_ Other Reasons

Policy

INTERNET SAFETY AND TECHNOLOGY

The Morris County Vocational School District 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 New Jersey state 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).

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/her designee.

The chief school administrator or his/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.

TECHNOLOGY (continued)

**The board designates the chief school administrator and or his/her designee as the coordinator of the district system. He/she shall recommend to the board of education qualified staff persons to ensure
provision of 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 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 Students

All students shall be granted individual e-mail accounts. An agreement will be required for an individual e-mail account and must be signed by the student and his/her parent/guardian.

Individual E-mail Accounts for District Employees

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.

District Web Site

The Board of Education authorizes the chief school administrator or his/her designee to establish and maintain a district web site. The purpose of the web site will be to inform the district

TECHNOLOGY (continued)

educational community of district programs, policies and practices.

Staff may also establish web sites that include information on the activities of that school or class. The District Technology Coordinator, program supervisors and the building principal shall oversee these web sites.

The chief school administrator or his/her designee shall publish and disseminate guidelines on acceptable material for these web sites. The chief school administrator or his/her designee 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 or his/her designee 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. 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 (hacking) 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.

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.

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.

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 pupils.

Privately-Owned Technology

The Board of Education recognizes technology is always changing and as a result of increased accessibility to technology many students possess technology devices for their use during non-instructional hours. These privately-owned devices may be beneficial to students during school hours for approved educational purposes. Therefore, the Board of Education will allow students to use their privately-owned technology devices and access the district Wi-Fi under conditions outlined in this policy.

The use of privately-owned technology by a student in the educational program during the school day must be approved by the student's parent or legal guardian and the school teaching staff member responsible for supervising and/or providing the students' instructional program. A teaching staff member may approve a student's use of privately-owned technology based on the assignment(s) to the student. The teaching staff member may also prohibit the use of privately-owned technology for an assignment(s).

Guidelines for Privately Owned Technology

1. Students and teachers must abide by the District Internet Acceptable Use Policy and Regulations, and are subject to all student code of conduct restrictions and disciplinary consequences relating to use or misuse of technology.

2. Students who use privately-owned technology in school will be given Wi-Fi access.

3. The teaching staff member, in considering the use of privately-owned technology, will ensure all students have equal advantage or benefit in completing an assignment(s). Students who do not have privately-owned technology will be furnished a school-owned device to insure equity when necessary.

4. Students may not use the camera or audio feature on their device to capture, record, or transmit audio, video or still photos of other students, faculty, or staff without explicit written permission given by the subject of the photo or video.

5. A teacher, staff member, or an administrator may request at any time that the privately owned electronic device be turned off and put away. Failure to do so may result in disciplinary action and revocation of access to the internet.

6. The school district assumes no responsibility for any privately-owned technology brought to school by a student. The student shall be responsible for the proper operation and use of any privately-owned technology brought to school. School staff members shall not be responsible for the effective use and/or technical support for any privately-owned technology. The school district shall assume no responsibility for the security of or damage to any privately-owned technology brought to school by a student. Students are encouraged to purchase private insurance for loss, damage, or theft of any privately-owned technology the student brings to school. A student who brings his/her device to school shall do so at his/her own risk. No searches or investigations will be conducted for lost or stolen devices beyond the normal operating procedures for a lost or stolen item. The district does not guarantee access to district provided internet access on personal devices. A student is solely responsible for all usage charges incurred at any time on their personal electronic device.

7. In the event that a student's official Individual Education Program (IEP) or Section 504 Rehabilitation Plan contains provisions for the use of assistive technology, including a privately-owned device, such provisions shall be taken into consideration when the District seeks to implement this policy.

Implementation

The chief school administrator or his/her designee may prepare regulations to implement this policy.

Adopted:	**December 12, 1996**
Revised/Readopted:	**April 3, 2003**
Revised/Readopted:	**September 9, 2003**
NJSBA Review/Update:	**February 2009**
Readopted:	**August 11, 2009**
Readopted:	**October 12, 2010**
Revised/First Reading:	**February 11, 2014**
Second Reading/Adoption:	**March 11, 2014**

Key Words

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

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	**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	

TECHNOLOGY (continued)

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)

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**
	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 and bullying**
***5131.5**	**Vandalism/violence**
***5142**	**Pupil 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.