

Policy

TECHNOLOGY RESPONSIBLE USE – NETWORKED SERVICES AND INTERNET

Policy and Purpose Statement

It is the goal of the West Morris Regional High School District to promote a shared passion for learning, academic excellence, involved citizenship, personal responsibility, and a respect for diversity; fostering the development of creative, confident, compassionate, and resilient individuals who contribute to their future communities. Access to and educational use of the information available from the Internet and other electronic communication sources is consistent with the goals and objectives of the district.

The West Morris Regional School District Board of Education believes that access to information through such sources as the Internet and email has become, if used appropriately, an integral part of the educational program. Therefore, 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.

It is the student's responsibility to access information specifically for educational purposes, and to use that information appropriately. Educational purposes are those that are related to the preparation and completion of classroom activities, assignments and other pertinent school business. For employees, this also includes purposes related to job performance. This Board Policy is intended to comply with the Children's Internet Protection Act, Children's Online Privacy Protection Act, and the Family Educational Rights and Privacy Act.

Although the Internet offers vast opportunities for accessing resources, the Board must also maintain an environment that promotes both responsible and ethical conduct in all activities engaged in by students and staff. Access to the internet, email services, and other forms of electronic communication bring the possibility, even with the use of filtering hardware and software, that materials may be accessed by students and staff that is either of no educational value, or violates applicable state or Federal law. With the current state of technology, it is impossible to control access to all materials that are obscene or profane, or advocate illegal acts, violence or unlawful discrimination.

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 chief school administrator shall develop procedures to determine other Internet material and/or access that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the chief school administrator or designee will develop and ensure education is provided to every student and staff member regarding appropriate online behavior, including interacting with other individuals on social networking sites and/or chat rooms, and cyber-bullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy: Policy 6142.10 Technology Responsible Use – Networked Services and Internet. Any changes in Policy 6142.10 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, technology labs and media centers in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

TECHNOLOGY RESPONSIBLE USE—NETWORKED SERVICES AND INTERNET (continued)

It is the belief of the Board of Education of the West Morris Regional High School District that the educational value of the access to information and the interaction enabled by Internet access and email far outweighs the potential disadvantages that may occur. The operation of the district computer network relies, in part, on the proper conduct of the users--students and staff. Therefore, it is necessary for students and staff to follow the guidelines which are set forth within this policy. If any user, whether a student or a staff member, violates this policy, his/her privileges to use the district network, devices or services may be limited or suspended. In addition, the student or staff member may be subject to other applicable disciplinary measures as per District policy, District Student Disciplinary Code, or statute.

Attached to this policy is a Student Technology Responsible Use Agreement. The agreement incorporates this policy as well as the Student Use of Privately Owned Technology Policy. It also indicates that the party who has signed the agreement has read the terms and conditions carefully and understands their significance. The user agreement is an acknowledgment of the responsibilities of all users. Students will not be permitted to use the district's network, devices or services unless they have signed the agreement and their parents or guardians have signed the agreement indicating the student has his/her permission to use the district network, devices and services. The agreement/permission form annexed to this policy is expressly made a part of the policy.

Terms and Conditions of Use**1. Responsible Use.**

The purpose of providing access to our computer network, devices, services, and email is expressly to support research and learning. It is to afford access to various resources and opportunities for collaboration, communication, creativity, and critical thinking. The use of the network, district devices, services, and email must be solely to support research and learning which furthers the educational objectives and curriculum established by the West Morris Regional High School District Board of Education. Whether accessing the district's network and services from outside school or not, all users are subject to the terms and conditions of this policy. The district expects that parents will supervise their child(ren) when using district technologies from home. In addition, the use of other organizations' networks or computer resources must comply with the rules for use of those networks in addition to those of this school district.

Transmission and accessing of any material in violation of any Federal law, state law or regulation/or Board Policy is prohibited. Prohibited activities include, but are not limited to the following:

- a. Students are prohibited from disclosing, either through email or via the Internet, personally identifiable information about any other individual such as addresses, phone numbers, pictures, email addresses, or the name and location of the school.
- b. The use of email distribution lists by students, including those created by the WMRHSD or by an outside party or individual, is strictly prohibited.
- c. District employees shall be provided with an email account and access to the system. District employees are required to use the district email system for any emails relating to school business. Staff members are prohibited from revealing, through email or via the Internet, any personally identifiable information for any individual such as name, address, telephone number, email address or picture, except as required for educational purposes. Staff emails that contain pertinent district information may be retained for up to 7 years.
- d. Users will not transmit or access material that is profane, obscene, harmful to minors (as that term is defined in the Children's Internet Protection Act), or advocates illegal acts, violence or unlawful discrimination.

TECHNOLOGY RESPONSIBLE USE–NETWORKED SERVICES AND INTERNET (continued)

- e. All users will be assigned a password. The password is to remain private and is not to be shared with other users.
- f. Any use of the network for commercial or for-profit purposes is prohibited.
- g. Use of the network for personal and private business is prohibited.
- h. Any use of the network for advertising or political purposes is prohibited.
- i. Users of the network shall not disrupt or interfere with the use of the network by others.
- j. The hardware or software shall not be altered, mishandled or abused in any way.
- k. In compliance with 5131.1, the district Harassment, Intimidation, and Bullying policy, the district network, devices and services shall not be used to harass others. Hate mail, discriminatory remarks, and cyber-bullying are prohibited.
- l. The installation of unauthorized software, whether copyrighted or shareware, for use on the district computer system is prohibited.
- m. Violation of the intellectual property rights of others is prohibited.
- n. Unauthorized gaming and/or gambling activities are prohibited.
- o. Accessing proxy avoidance sites is prohibited.

2. Privileges

- a. The use of the district's network, devices, services, and email is a privilege, not a right. Inappropriate use may result in the suspension, or partial suspension of those privileges as well as other possible discipline as outlined in the District Student Disciplinary Code and District policy, and even possible prosecution for illegal activity.
- b. Staff members shall also be subject to appropriate discipline, dismissal and/or prosecution for illegal or prohibited activity. Staff members are responsible for following the provisions of this policy as a condition of their employment.
- c. Each student, in order to obtain access to the network and district services will be required to complete the West Morris Regional High School District Student Technology Responsible Use Agreement annually. The chief school administrator or his/her designee will have the authority to, at least temporarily, suspend use of the network and services at any time.
- d. If a student or staff member chooses to bring their own device or technology they must comply with all guidelines referenced in 6142.11 Student Use of Privately Owned Technology.

3. Network Etiquette. Users of the district computer system and network(s) are expected to:

- a. Be polite.
- b. Use only appropriate language.
- c. Be prepared for periodic searches of student or staff files and other electronic storage areas. The chief school administrator or his/her designee may access these files from time to time not only to insure system integrity, but also to determine if users are complying with this policy. Users should not expect that information either transmitted or stored on the network or district services will be private.

TECHNOLOGY RESPONSIBLE USE–NETWORKED SERVICES AND INTERNET (continued)

- d. Comply with all intellectual property laws, such as copyright and fair use.
- e. Users should disclose to an administrator, teacher or parent any information or electronic messages that make them uncomfortable.

Security and Vandalism

Security of the network is a high priority. If a user has reason to believe that they can identify a security problem with the network, district devices or services, they must notify the District Coordinator of Technology Integration, Network Administrator or Systems Administrator.

Vandalism will result in the automatic suspension of use and will be subject to discipline, other forms of legal action or perhaps even criminal prosecution. Vandalism is defined as any attempt to harm, steal or destroy data, software or hardware, even if belonging to another network. This includes, but is not limited to, the creation of a virus, intentional propagation of a virus, or dissemination of contaminated storage devices such as flash drives and optical disks.

Users will be personally charged and held responsible for any costs related to damages to district technologies caused by intentional misuse, lack of care and/or reasonable precautions.

The West Morris Regional High School District makes no warranties of any kind, whether express or implied, for the service it is providing. The district will not be responsible for any damages users suffer. This includes loss of data, non-deliveries, mis-deliveries, or service interruptions caused by the district's own negligence or the user's errors or omissions. The district cannot accept responsibility for the accuracy or quality of information obtained through its network and/or services. **Therefore, the West Morris Regional High School District will not be held responsible for any inappropriate material acquired from this network.**

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.

Implementation

The chief school administrator shall prepare regulations to implement this policy.

NJSBA Review/Update:	April 2011, April 2018
Adopted:	February 27, 2012
Revised:	February 11, 2013
Revised:	June 27, 2016
Revised:	December 10, 2018

TECHNOLOGY RESPONSIBLE USE–NETWORKED SERVICES AND INTERNET (continued)Key Words

Responsible Use, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web

Legal References: N.J.S.A. 2A:38A-1 et seq. Computer System
N.J.S.A. 2A:38A-3 Federal Communications Commission: Children's
Internet Protection Act.
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:30-1.1 et 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
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.