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. 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.

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. 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.

c. 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.

d. All users will be assigned a password. The password is to remain private and is not to be shared with other users.

e. Any use of the network for commercial or for-profit purposes is prohibited.

f. Use of the network for personal and private business is prohibited.

g. Any use of the network for advertising or political purposes is prohibited.

h. Users of the network shall not disrupt or interfere with the use of the network by others.

i. The hardware or software shall not be altered, mishandled or abused in any way.

j. 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.

k. The installation of unauthorized software, whether copyrighted or shareware, for use on the district computer system is prohibited.

l. Violation of the intellectual property rights of others is prohibited.

m. Unauthorized gaming and/or gambling activities are prohibited.

n. 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. 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.

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.**

Implementation

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

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

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.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

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.

STUDENT USE OF PRIVATELY-OWNED TECHNOLOGY

The Board of Education recognizes technology is constantly changing and as a result of increased availability, the manner in which digital content is accessed, communicated and transferred has vastly transformed the consumption of information. Privately Owned Devices provide students and teachers with educationally pertinent content, information and resources that can have a positive impact on teaching and learning. Therefore, the Board of Education will allow students to use their privately-owned technology devices and access the WMRHSD Wi-Fi under conditions outlined in this Policy. **It is important to note that connecting to the WMRHSD Wi-Fi network with privately-owned technology is a privilege, not a right for district students.**

For the purpose of this policy:
- "technology" means hardware or software.
- "privately-owned" means technology hardware and software that is purchased, owned, and maintained by the student at no expense to the school or school district.
- "hardware" means any device that can store, access, retrieve, and/or communicate data or information. "Hardware" may include, but is not limited to, any type of computer device; smart phone; tablet, electronic e-reader; video broadcasting and/or recording device; or camera.
- "software" means any application (app) or program that provides instruction for telling a computing device what to do and how to do it.

The Board also recognizes privately-owned technology allows students to access sources of information that have not been pre-screened by educators using Board approved standards. The Board therefore adopts the following guidelines for the use of personal electronic devices and declares unethical, unacceptable or illegal behavior as just cause for taking disciplinary action, limiting or revoking Wi-Fi access privileges, and/or instituting legal action. **The student's parent or legal guardian and the school teaching staff member responsible for supervising and/or providing the student's instructional program must approve the use of privately-owned technology by a student in the educational program during the school day.**

Guidelines for Privately Owned Technology Use

1. Students and teachers must abide by the District Responsible Use Policy, 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 not be given access to the school district's computer server(s) and any network(s) except for the guest segmented Wi-Fi. Students may not connect privately-owned technology devices to District owned hardware using USB connections, unless they have specific written permission from the District Coordinator of Technology Integration.

3. A teaching staff member who approves a student to use their privately-owned technology to access the Internet during instructional time will provide the student with a specific set of parameters for how said device is to be utilized. A student granted such permission must comply with school district policies and regulations regarding acceptable use of computers and technology. Any use of privately-owned technology by a student shall be in strict accordance with the teaching staff member's specific approval(s) and Board policies and regulations. Any violation will subject the student to appropriate discipline and/or grading consequences.

4. The teaching staff member, in considering the use of privately-owned technology, will ensure such approval does not provide any advantage or benefit to the student who owns such technology over the

student who does not own such technology. The teaching staff member will not approve the use of privately-owned technology if the teaching staff member determines the use would be advantageous or beneficial to the student who owns such technology over the student who does not own such technology.

5. 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.

6. 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 district's Wi-Fi network.

7. 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.

8. In the event that a student's official Individualized Education Program (IEP) or Section 504 Accommodation 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.

Adopted: January 7, 2013
Revised: June 27, 2016

Privately-Owned Technology Guidelines and Rules

Purpose

The West Morris Regional High School District ("WMRHSD") will allow students in grades 9-12 to use privately-owned technology to access the WMRHSD wireless guest network. In an effort to leverage student-owned technology for educational purposes, the WMRHSD will allow personal devices on our network and school grounds for students who follow the responsibilities stated in the Responsible Use Policy and the following guidelines regarding privately-owned technology.

WMRHSD provides technology and devices that are appropriate and relevant to support instructional purposes. **The use of personal electronic devices by students is optional.**

An important component of allowing students to use privately-owned technology will be education about appropriate online behaviors. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviors. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal electronic devices.

Allowed Device Types

For the purpose of this program, "devices" will include: laptops, cell phones, smartphones, eReaders, iPads, iPods, and tablets. **Handheld gaming devices are not allowed.**

Guidelines

1. Students and parents/guardians must adhere to the Student Code of Conduct, Student Handbook, Technology Responsible Use Policy (6142.10), and all Board policies, particularly Student Use of Privately-Owned Technology (6142.11), which are available on the district website: www.wmrhsd.org.
2. Teacher permission is necessary for student use of privately-owned technology. Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and for use during a specific timeframe.
3. Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher.
4. Devices may not be used to cheat on assignments or tests or for non-instructional purposes (such as making personal phone calls and text/instant messaging).
5. Students may not use devices to record, transmit, or post photographic images, audio or video of a person or persons on campus during school activities and/or hours, without written consent from a teacher and for specific instructional purpose(s).
6. Devices may only be used to access the Internet and district's services that are relevant to the classroom curriculum.

Students and Parents/Guardians acknowledge that:

1. The school's network filters will be applied to a device's connection to the Internet and any attempt to bypass the network filters is prohibited.
2. Students are prohibited from:
   a. Bringing a device on premises that infects the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
   b. Processing or accessing information on school property related to "hacking," altering, or bypassing network security policies.

3. WMRHSD is authorized to collect and examine any device that is suspected of causing technology problems or that was the source of an attack or virus infection.
4. Printing from personal laptops or devices will not be possible at school.
5. Personal devices must be charged prior to school and run on battery power while at school
6. Voice, video, and image capture applications may only be used with prior written teacher permission and for specific instructional purpose(s).
7. The teacher 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 network.
8. WMRHSD reserves the right to examine the privately-owned electronic device and search its content if there is reason to believe that WMRHSD policy or local state and/or federal laws have been violated. In the event that a student believes that his/her password has been compromised, he/she should immediately inform their teacher or administrator.

Lost, Stolen, or Damaged Devices

Each user is responsible for his/her own digital property and should treat it and use it responsibly and appropriately; WMRHSD takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

Usage Charges

WMRHSD cannot be held responsible for any possible device charges to your account that might be incurred during approved school-related use.

Network Considerations

Users should strive to maintain appropriate bandwidth for school-related work and communications. **Access to the guest Wi-Fi is provided for electronic communication and light web-browsing only**.

WMRHSD does not guarantee connectivity or quality of connection with personal devices, but will provide trouble-shooting documentation about how to connect with a variety of operating systems and devices.

Adopted: June 27, 2016

6142.10 FORM

WEST MORRIS REGIONAL HIGH SCHOOL DISTRICT

6142.10 - STUDENT TECHNOLOGY RESPONSIBLE USE AGREEMENT

This form is to be completed by students after reviewing the district Technology Responsible Use Policy, Student Use of Privately-Owned Technology Policy and all documents incorporated by reference. The completion of this form indicates that you have read the policy and understand the same. It also indicates that you agree to abide by the terms and conditions of the policy. Regardless of your age, this form must be signed both by you and a parent/guardian before you will be permitted to have access to the district's network, services and devices.

I understand and agree to accept and abide by the Technology Responsible Use Policy. I also understand that if I fail to follow the policy, my access to the district's network, services and devices may be suspended. I may be subject to other discipline, and there may even be criminal consequences to my behavior depending upon the severity of my actions.

Student Signature: _____ Date: _____

Name (please print): _____

School: _____ Grade: _____

As a parent/guardian of the student, above, I hereby give my permission for my child to access the district's network, services and devices, including email. I have read the district Technology Responsible Use Policy and Student Use of Privately-Owned Technology Policy, and I understand that my child is expected to abide by same. I understand that the district is employing filtering software, but that it is not always effective. I also understand that when my child is accessing the district's network and/or services from outside of school, I am responsible to provide appropriate supervision.

Parent/Guardian Signature: _____ Date: _____

Name (please print): _____

Complete and return to your child's high school Technology Department.

2/11/13

Reviewed/revised: June 27, 2016

Technology Signature Page

Student Name: _____ Circle Class: 2017 2018 2019 2020

I have read, understand and agree to abide by the rules, terms, and conditions of West Morris Regional High School District's 6142.10 Technology Responsible Use- Networked Services and Internet Policy. I further understand that any violation of this policy is unethical and may constitute a criminal offense. I understand that any violation of the policy could result in the revocation of my access rights, the imposition of school discipline criminal prosecution and other legal action.

Name of Student User (print): _____

Student/User Signature: _____ Date: _____

Parent/Guardian Consent

(If user is under the age of 18, a parent or guardian must also read and sign this agreement.)
As the parent/guardian of this student, I have read and reviewed the district's 6142.10 Technology Responsible Use Networked Services and Internet Policy. I understand that this access is designed for educational purposes and the West Morris Regional High School District has taken precautions to eliminate controversial materials, and I will not hold the district responsible for materials used, viewed, or acquired on the network.
Further, I understand that improper or inappropriate use of the network by my child could result in school discipline, criminal and civil penalties. I accept full responsibility for any damages or injuries caused by my Child's use of the network, either in or outside of school, in a manner which violates the Rules, Terms, and agreements set forth by this policy.

With this understanding, I herby give permission to issue electronic network and Internet access for my child and certify the information on this form is correct.

Parent/Guardian (print): _____

Signature of Parent/Guardian: _____ Date: _____

++

Privately-Owned Technology Responsible Use Guidelines

I recognize it is impossible for the school to restrict access to all controversial materials, and I will not hold the school responsible for materials acquired on the school network. I understand that children's computer activities at home should be supervised as they can affect the academic environment at school.

I understand and will abide by the above guidelines and by those set forth in the WMRHSD Technology Responsible Use Policy (6142.10) and Student Use of Privately Owned Technology Policy and Regulation. (6142.11). I further understand that any violation is unethical and may result in the loss of my network and/or device-privileges as well as other disciplinary and or legal action.
I also understand that my school network is owned by WMRHSD and is not private.
I understand and will abide by the above policy and rules.

DEVICE(S) THAT STUDENT WILL BE USING AT SCHOOL:

Parent/Guardian Signature: _____ Date: _____

Name (please print): _____

Student Signature: _____ Date: _____

Name (please print): _____

☐ I DO NOT WISH TO BRING PRIVATELY-OWNED TECHNOLOGY TO SCHOOL.

Parental/Guardian Consent Form

We are sending you this parental consent form to both inform you and to request permission for your child's photo/image and personally identifiable information to be published on the district and/or school's website.

As you are aware, there are potential dangers associated with the posting of personally identifiable information on a web site since global access to the Internet does not allow us to control who may access such information. These dangers have always existed; however, we as schools do want to celebrate your child and his/her work. The law requires that we ask for your permission to use information about your child (see information below).

Pursuant to law, we will not release any personally identifiable information without prior written consent from you as parent or guardian. Personally identifiable information includes student names, photo or image, residential addresses, e-mail address, phone numbers, and locations and times of class trips.

If you as the parent or guardian, wish to rescind this agreement, you may do so at anytime in writing by sending a letter to the principal of your child's school and such rescission will take effect upon receipt by the school.

Check One of the Following Choices:

☐I/We GRANT permission for a photo/image that includes this student without any other personal identifiers to be published on the school and/or district's public Internet site.

☐I/We GRANT permission for this student's photo/image and name to be published on the school and/or district's public Internet site.

☐I/We GRANT permission for this student's photo/image and all other personal identifiers listed above to be published on the school and/or district's public Internet site.

☐I/We DO NOT GRANT permission for photo/image that includes this student to be published on the school and/or district's public Internet site.

Student's Name: (please print) _____ Student's Grade: _____

Print name of Parent/Guardian: (print) _____

Signature of Parent/Guardian: _____

Relation to Student: _____

Date: _____

Bill A592: Prohibits Dissemination of Personal Student Information on the Internet Without Parental Consent

On January 8, 2002, Bill A592, as listed below, was passed by the legislature.
Be It Enacted by the Senate and General Assembly of the State of New Jersey:

The board of education of each school district and the board of trustees of each charter school that establishes an Internet web site, shall not disclose on that web site any personally identifiable information about a student without receiving prior written consent from the student's parent or guardian on a form developed by the Department of Education. The written consent form shall contain a statement concerning the potential dangers of personally identifiable information about individual students on the Internet.

As used in this act, "personally identifiable information" means student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.

This act shall take effect immediately.