

WEST MORRIS REGIONAL HIGH SCHOOL DISTRICT

STUDENT ACCEPTABLE USE POLICY

COMPUTER NETWORK AND TECHNOLOGY RULES, TERMS AND CONDITIONS REGARDING STUDENT USE OF THE COMPUTER NETWORK AND INTERNET RESPONSIBILITY

Please read the following carefully before signing this document. This is a legally binding document and must be signed before you will be given access to the district's electronic network and Internet. The West Morris Regional High School District's Technology Network is designed to increase student access to a variety of learning tools and, with that access; there is the need to establish responsibilities.

If any user violates any of the following provisions, discipline procedures will be enforced in order to protect the district's network system. In addition, the parent and/or student may be held liable for monetary damages for unauthorized or improper use, damage or vandalism. The signatures at the end of this document are legally binding and indicate that the parties who signed have read the rules, terms and conditions carefully and understand their significance.

Rules, Terms and Conditions

1. **Acceptable Use:** The purpose of the district's computer network is to support research and learning by providing students with an account that may be accessed on any computer in the system that is connected to the network. In addition, the use of this network is to assist in preparing students for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to interact globally. The use of the district's network must be in support of education and research and consistent with the educational objectives of the West Morris Regional High School District. The use of the district's network is a privilege, not a right, and inappropriate use (as outlined in this contract) may result in cancellation of those privileges.

2. **Unacceptable Use:**

(a) **While utilizing any portion of the electronic network, unacceptable behaviors include, but are not limited to, the following:**

- Students will not post information that, if acted upon, could cause damage or danger of disruption.
- Students will not engage in personal attacks, including prejudicial or discriminatory attacks.
- Students will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending messages, they must stop.
- Students will not knowingly or recklessly post false or defamatory information about a person or organization.
- Students will not use criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Students will not use speech that is inappropriate in an educational setting or violates district rules.
- Students will not abuse network resources such as sending chain letters or "spamming."
- Students will not display, access or send offensive messages or pictures.
- Students will not use the electronic network for commercial purposes. Students will not offer, provide, or purchase products or services through this network.
- Students will not use the electronic network for political lobbying. Students may use the system to communicate with elected representatives and to express their opinions on political issues.
- Students will not attempt to access non-instructional school/district systems, such as student information systems or business systems.
- Students will not use of any wired or wireless network (including third party internet service providers) with equipment brought from home. Example: The use of a home computer on the network or accessing the internet from any device not owned by the district.
- Students will not use district equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.

- Students will not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

The following is a list of graduated disciplinary actions. However, the severity of any violation will be considered and this may negate any stepped action and invoke actions that may include other school and/or police measures. Any incident that involves school equipment in a bullying and/or harassment issue may include additional time to be locked out from the network and will involve the police. The discipline code is as follows:

First offense: A student is locked out of the network for a minimum of one week. He must report to the appropriate Assistant Principal and fill out a request to be reinstated.

Second offense: A student is locked out of the network for a minimum of two weeks. He or she must report to the appropriate Assistant Principal and fill out a request to be reinstated.

Third offense: A student is locked out of the network for a minimum of four weeks. A discipline referral with mandatory parent conference is required. A computer network lockout will be in effect until the parent conference has taken place.

If the offense is such that it denies lab use by others, the student may be locked out of the district network for the remainder of the year. In addition, if the offense causes a significant disruption in the use of the computers or network by others, it may also constitute "damage" under the paragraph below and the offense accordingly upgraded to a level with appropriate additional penalties.

(b) Damage to Software, Hardware or Peripherals. This may include, but is not limited to the following:

- Physical tampering or altering hardware/software configuration
- Deleting files outside of the personal directory
- Loading and executing a virus program on any workstation
- Defacing equipment
- Taking equipment or disks
- Removing or changing cable connections
- Acquiring unauthorized system rights or access for oneself or others
- Interfering with teacher/student material on the network
- Downloading or copying files or programs from the system without authorization or copying any files in violation of copyright laws
- Any other action which damages files, software, hardware or peripherals and results in a disruption in the use of the computers or network by others
- Any form of "hacking" which may include the use of software

All offenses: Any damage to software, hardware or peripherals is considered damage to school property for which adult students, and the parents of minor students, will be held financially responsible in accordance with the law, including NJSA 18A:37-3. Adult students and/or the parents of minor students will be charged for all labor and/or parts required to repair the damage, regardless of whether the problem is repaired using in-house personnel or an outside vendor. The student shall be denied access until payment is received and may also be denied access for a period of up to one calendar year.

Where an offense may also constitute a violation of criminal laws (e.g., theft of copyright materials, making threats against others, destruction of property), the matter may also be referred to the police, courts or juvenile justice authorities.

Floppy Disk/CD-ROM/Flash Drive Policy

Students are not permitted to place their own disks/CD-ROMs/flash drives into any district drive without first obtaining explicit permission from a teacher. That teacher must be informed of all files that will be transferred from the network to the student's disk/CD-ROM/flash drive. Any student who places files on the system without permission will be subject to disciplinary procedures. If a virus or any damaging files are placed on the system, the student responsible will pay for the repairs at the rate set by the school Technology Assistant.

Note: These procedures will be implemented in conjunction with applicable Discipline Codes and Code of Behavior Infractions contained in the Student Handbook. It is understood that each case of inappropriate use is subject to administrative review to determine if there is a need for further action.

3. Services: The West Morris Regional High School District will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries or service interruptions caused by system network failure or your errors or omissions. Use of any information obtained via the district's network is at your own risk. The West Morris Regional High School District denies any responsibility for the accuracy or quality of information obtained through its services.

4. Updates: The West Morris Regional High School District may occasionally require new registration and account information from you to continue providing services. All Rules, Terms and Conditions as stated in this document are applicable to the West Morris Regional High School District. These Rules, Terms and Conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These rules, terms and conditions shall be governed and interpreted in accordance with the laws of the State of New Jersey, United States of America.

5. Plagiarism: Plagiarism, the sharing of electronic files is prohibited. These issues will be addressed as violations of both the ***Rules of Acceptable Technology Use*** and ***Academic Honesty***. The District **has employed a service** that will scan the Internet for suspected plagiarized information.

6. System Security

- Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should students provide their password to another person.
- Students must immediately notify a teacher or the system administrator if they have identified a possible security problem. Students should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Students will not attempt to gain unauthorized access to any portion of the electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Students will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
- Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
- Users will not use sniffing or remote access technology to monitor the network or other user's activity.
- Software is available to students to be used as an educational resource. No student may install, upload or download software without permission from the district technology department.
- Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of the electronic network may lead to discovery that a student has violated this policy or the law. Students should not expect that files stored on district servers are private.

WEST MORRIS REGIONAL HIGH SCHOOL DISTRICT

INTERNET RESPONSIBILITY

West Morris Central and West Morris Mendham High Schools contain access to the Internet. The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual people. The district's access allows for the following: (1) access to electronic mail (e-mail accounts for students are not supplied by the District); (2) information and news from a variety of sources and research institutions; (3) access to many university libraries, the Library of Congress, electronic research tools and the availability of school library resources from home computers.

With access to computers and people all over the world also comes the availability of some material that may not be considered to be of educational value within the context of the school setting. The West Morris Regional High School District has taken every available precaution to restrict access to inappropriate materials. An electronic filtering device is part of our network infrastructure and users may be monitored

However, on a global network, it is impossible to control all materials. The users of the District's access to the Internet firmly believe that the valuable information and interaction available on this worldwide network far outweigh the possibility of users procuring material that is not consistent with the educational mission of this district.

Following are guidelines provided to establish the responsibilities you are about to acquire. If any user violates any of these provisions, his or her access to the district's account will be denied. The signatures at the end of this document are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

Terms and Conditions

1. **Acceptable Use:** The purpose of the Internet is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of the district's account must be in support of education and research and consistent with the educational objectives of the West Morris Regional High School District. Transmission of any material in violation of any U.S. or state regulations is prohibited. This includes but is not limited to: copyrighted material, threatening e-mails or materials, slanderous or obscene e-mails or material and material protected by trade secret. Use for commercial activities by for-profit institutions is not acceptable. Use for product advertisement or political lobbying is also prohibited.

2. **Privileges:** The use of the district's Internet access is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. Only those students who have signed this contract shall be authorized to use the Internet. **Periodic monitoring of student Internet traffic and student selected sites will be conducted by the appropriate school official.**

3. **Network Etiquette:** The use of the district's account requires that you abide by accepted rules of network etiquette. These include, but are not limited to, the following:

- Be polite. Do not send abusive and/or threatening messages to anyone. Messages/e-mails of a threatening nature may involve the local police or other appropriate authorities.
- Use appropriate language. In all messages, do not swear or use vulgarities or any other inappropriate language. Anything pertaining to illegal activities is strictly forbidden. Messages relating to support of illegal activities must be reported to appropriate authorities.
- Privacy. **Do not reveal your personal address or phone numbers or those of any other person.** All communications and information accessible via the network should be assumed private property. **Never make arrangements to meet in person anyone who you do not know but have made contact with through the Internet.**
- Connectivity. Do not use the network in such a way that would disrupt the use of the network by others.
- Communications via the Internet are as good as saying it in person. **You will be held accountable for what is communicated by you to others.**

4. **Electronic Images:** Students may not take an electronic image of another student, staff member or any employee with out prior written consent. This is not only a school policy by a requirement from the State of NJ. There could be serious legal consequences if any images taken in a school are transmitted electronically or in print to others. This includes any pictures/video taken on a cell phone.

5. **Services:** The West Morris Regional High School District will not be responsible for any damages you may suffer. This includes loss of data resulting from delays, non-deliveries or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained via the district's account is at your own risk. The West Morris Regional High School District denies any responsibility for the accuracy or quality of information obtained through its services.

6. **Vandalism:** Vandalism will result in cancellation of privileges. This includes, but is not limited to, the uploading of computer viruses.

7. **Updates:** The West Morris Regional High School District may occasionally require new registration and account information from you to continue providing services. All Terms and Conditions as stated in this document are applicable to the West Morris Regional High School District. These Terms and Conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of New Jersey, United States of America.