



**Memorial Middle School
Acceptable Use Policy Form**
Please return this portion to the school.

School Year 2016-2017

Parent/Guardian Consent:

I have read and understood the **Acceptable Use Policy** for Spotswood Public Schools. I also have read and discussed with my child the implications of the student use agreement and the penalties involved for violating the agreement and have witnessed my child signing the document. I also understand the district technology is for educational purposes only and that the school district has taken reasonable steps to safeguard the access for users. However, I understand that it is not possible to stop all inappropriate activities and I will not hold the district responsible for any materials obtained through the use of the networks.

I give permission for my child to use all the technological resources of the Spotswood Public Schools.

Student User's Name: _____

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

**** This form will be valid for the years that your child is enrolled in his/her current school. If at any time you change your mind, you are welcome to update your form.**

ACCEPTABLE USE OF TECHNOLOGY

Purpose

Spotswood Public Schools provides students and staff access to a district electronic network, which includes: computer equipment, Internet access, and other technology related resources. The purpose of this network is to avail our students and staff access to millions of sources of information, which are presently available via the World Wide Web.

The students, staff, and community members of Spotswood Public Schools have the privilege of access to numerous technological resources for the specific purpose of improving and promoting the educational mission, goals and objectives of the district. This document serves to regulate and guide students and staff on the proper use of the district electronic network for the purpose of promoting the use of technology for educational use.

Limitation of Liability

The Internet constitutes a quasi-regulated collection of resources that change constantly, so it is not possible to totally predict or control the resources that users may locate. The Spotswood Board of Education 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 electronic network system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor and regulate all access to and use of the district network system including the district web site and the Internet.

The board designates the chief school administrator as the coordinator of the district network 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 network system, 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.

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 district network system. Sanctions for student improper use 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 and/or dismissal 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 as per state and federal regulation.

World Wide Web

Access to the Web is a privilege granted by the Spotswood Board of Education to all students and staff. Violation of this agreement will be met with loss of access privileges as per building administrations discretion. Access to the Web will be through the District's computers and access points. Private access to the Web via the district's network is not allowed.

Supervision of Students

Qualified staff shall supervise student use of the Internet for the sole purpose of promoting the district mission, goals and objectives. All other uses are prohibited.

District Web Site

The board authorizes the chief school administrator 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.

Individual schools and classes may also establish web pages within the district site that include information on the activities, assignment, and events of that school or class. The building principal shall oversee these web sites.

Parental Notification and Responsibility

The chief school administrator 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 use computer technology, incorporated within the district's "Acceptable Use Agreement." Parents/guardians who do not wish their child(ren) to have access to the district electronic network must notify the principal in

writing. Alternate assignments will be created for students who do not wish to participate and for those who loose privileges to accommodate their educational needs.

Acceptable Use: The six areas, which follow, are incorporated within the District's "Acceptable Use Agreement."

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 to the District system or to any other computer system through the district system shared or private files, 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", keyloggers, trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not purposely or maliciously destroy or deface equipment, peripherals, data, or software.

Users shall not use the district system to engage in illegal activities as outlined in federal and state law and network provider policies and licenses.

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 vandalize the account, work, or data of another user or organization.

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.

Users shall not utilize technology for the personal financial or business gain.

Users shall not install or use personal software or change the configuration of any individual computer or network.

Users shall not utilize file-sharing programs to promote copyright infringement.

Prohibited Language

Prohibited language applies to public messages, private messages, blogs, chat rooms, videoconferences, and material posted on district web pages accessed via the district network system.

Users shall not access, upload, download, or distribute pornographic, obscene or sexually explicit materials.

Users shall not send or receive messages or obtain materials that contain obscene, profane, lewd, vulgar, rude, inflammatory, bullying 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 or login with their account for another user. The sharing of access information is a violation of this agreement and will be met with disciplinary action and loss of privileges.

Users shall immediately notify the supervising staff person or building administration 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 technology staff.

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.

Users shall check e-mail frequently and delete messages promptly.

Privacy Rights

Users shall respect the privacy of messages that they receive and reposting messages without the approval of the sender is prohibited.

Users shall not publish private information about another individual.

The District's electronic mail system is the sole property of the District, and is principally intended for communications by staff and students directly related to the educational mission of the District. The Administration reserves the right to access any and all communications sent to or from the District's electronic mail system at any time, without prior notice. Accordingly, users should have no expectation of privacy in any communication sent to or from them on the District's electronic mail system.

Implementation

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

Adopted: April 29, 2003

Legal References:

N.J.S.A. 2A:38A-1 et seq.

N.J.S.A. 2C:20-25

N.J.S.A. 18A:7A-11

N.J.A.C. 6A:24-1.1 et seq.

See particularly:

N.J.A.C. 6A:24-1.4,2.2,4.1,6.1

N.J.A.C. 6A:30-1.1 et seq.

17 U.S.C. 101

47 U.S.C. 254(h)

N.J. v. T.L.O. 469 U.S. 325 (1985)

O'Connor v. Ortega 480 U.S. 709 (1987)

Manual for the Evaluation of Local School Districts (August 2000)

Computer System

Computer Related Theft

Annual report of local school district;
contents; annual report of commissioner;
report on improvement of basic skills
Urban Education Reform in the Abbott
Districts

Evaluation of the Performance of School
Districts

United States Copyright Law

Children's Internet Protection Act

Possible Cross References:

*1111	District publications
*3514	Equipment
3543	Office Services
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	Pupil safety
5145.2	Freedom of speech/expression
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.