No. **256**

SECTION: **STUDENTS**

TITLE: ACCEPTABLE USE OF DISTRICT INFORMATION AND TELECOMMUNICATIONS RESOURCES BY STUDENTS

Wissahickon School District
Ambler, Pennsylvania 19002

FIRST READING: June 14, 2010
SECOND READING: August 16, 2010
ADOPTED: August 16, 2010
REVISED:

1. Purpose

It is Board policy that the use of any and all information and telecommunications resources accessed through the Wissahickon Network Services (WNS) will be legal, in adherence with standards of the District and the community, and solely for educational purposes which are consistent with the curricular goals of the District.

2. Definitions

The term **educational purpose** includes use of the system for classroom activities, professional or career development, limited high-quality self-discovery activities, and administrative application.

This policy is referred to herein as the "Student Acceptable Use Policy."

3. Guidelines

General

This policy and these guidelines shall apply to all student users who obtain access privileges to or otherwise access networks and/or telecommunications systems, which are entered via equipment and access lines housed, operated or maintained by or for the District. In addition, this policy shall, where applicable, apply to the use of all District information and telecommunications resources, whether connected to an electronic network or operated on a "stand alone" basis and to the access to information networks and services provided to the user by or through the District, regardless of the location or ownership of the equipment through which a network or service is accessed.

Accounts for accessing all information and telecommunications resources and electronic networks maintained by or for the District ("internal networks"), or other networks which may be accessed through the District internal networks, will be provided to users solely for educational purposes which are consistent with the curricular goals of the District.

The use of WNS is a privilege, not a right, and may be revoked by the Superintendent or his/her designee at any time for abusive conduct or violation of the terms of this policy or the administrative regulations accompanying this policy.

The District cannot warrant what functions of the system and network will meet any specific requirements, or that systems operations will be error free or uninterrupted. The District shall not be liable for any direct, incidental, or consequential damages sustained or incurred in conjunction with the use, operation or inability to access or use WNS, including the loss of data, information or anything else of value which the user seeks to maintain or derive through the network. The District shall not be liable for any damage incurred due to harmful programs or materials, including but not limited to computer viruses, which may be accessible or propagated through the WNS.

Electronic mail (E-mail) accounts and other forms of electronic communication provided by or through WNS are not private. The Superintendent or his/her designee and the Director of Technology may access e-mail and other forms of communication at any time, and E-mail software may be utilized to misdirect messages if so designated. Users should be aware of these limitations when communicating with others.

The reposting of personal communications to public spaces without the original author's prior specific consent is prohibited. However, communications which are accessible in a public forum may be copied in subsequent communications, as long as proper reference is given to the original author of the copied information.

Use of WNS or its hardware or software components for any activities which may be criminal under local, state, or federal law is expressly prohibited, including but not limited to usage involving vandalism or destruction of, tampering with or unauthorized entry into computers, files or software. The District will cooperate fully with local, state, and federal officials in any investigation conducted concerning or related to alleged illegal activities of any individual involving the misuse of the WNS.

Parental Notification and Responsibility

The Superintendent shall implement a program, which educates students about the risks and consequences associated with the use of the WNS. The District will notify the parent or legal guardian about the WNS and the policies governing its use. A parent or legal guardian must sign a Student Internet Permission Form to allow their child to have an individual account accessed through WNS. Parents or legal guardians may request alternative activities for their child that do not require Internet access.

This Student Acceptable Use Policy expressly prohibits the accessing of inappropriate material. A wide range of material is available on the Internet, some of which may not be consistent with educational purposes which are consistent with the curricular goals of the District. The District will use appropriate content and access filtering software. However, no filtering software is completely effective to prevent access to inappropriate material. The District reserves the right to monitor and restrict the content of all materials that students might access with using WNS and/or District equipment, and will reasonably attempt to ensure that inappropriate content is blocked or filtered. The District reserves the right to prohibit access to any website sought by users. However, it is not practically possible for the District to monitor and enforce a wide range of social values in student use

of the Internet. Further, the District recognizes the parents or legal guardians bear the primary responsibility for transmitting their particular set of family values to their children. The District encourages parents or legal guardians to specify to their child what material is and is not acceptable for their child to access through the WNS, as consistent with this policy.

The District will provide students and parents or legal guardians with guidelines for student safety while using the Internet.

Parents or legal guardians are responsible for monitoring their student's use of the Internet when they are accessing the system from home.

District Limitation of Liability

The District does not warrant, either express or implied, that the functions or the services provided by or through the WNS are error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data, interruptions of service and/or the inability to access WNS. The District is not responsible for financial obligations and/or issues arising through the unauthorized use of the system or due to other unauthorized or improper acts. Users will fully indemnify the District against any damage incurred by the District caused by the use of the WNS in violation of this policy.

Due Process

The District will fully cooperate with local, state, and federal officials in any investigation concerning or relating to any alleged illegal activities conducted through the District system. The District reserves the right to provide appropriate access to outside consultants who are retained to address a WNS issue.

In the event there is an allegation that a student has violated the Student Acceptable Use Policy, the student will be provided with notice of the alleged violation and be given an opportunity to present an explanation and any accompanying information related to the alleged violation.

Disciplinary actions will address the specific concerns arising from the alleged violation of this policy and to assist the student in gaining the self-discipline necessary to appropriately use WNS.

A student's account(s) through WNS will be revoked immediately following the student's withdrawal or expulsion from the District.

The Superintendent or his/her designee and the Director of Technology may revoke the WNS usage privileges of a guest user at any time and shall provide notice to the user of such revocation. Guest accounts which are not active for more than thirty (30) days may be terminated, along with the user's files, without notice to the user.

Search and Seizure

WNS users, including students, have no privacy expectation in the contents of their personal files on the WNS.

Routine maintenance and monitoring of the system may lead to the discovery that a user has or is violating the Student Acceptable Use Policy, another District policy, or federal, state and/or local law. Documentary and other evidence which is discovered on WNS may be used in any investigation or disciplinary action against a student user who has allegedly violated a District policy and/or the law.

An individual search may be conducted if reasonable suspicion exists that a user has violated the law or the District policies. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

System users have no privacy expectation regarding what appears on their screen at any given time. The District reserves the right at all times to use a remote access feature, which enables authorized District employees and other authorized individuals to view what appears on a user's monitor when the user is utilizing WNS.

Copyright

The Board affirms that respect for personal property, whether tangible or intangible, is vital to maintaining an appropriate learning and working environment. The Board will establish and the Superintendent will enforce a copyright policy for student users.

Students are required to comply with copyright law and the District's copyright policy. Any student who violates a copyright law and/or the District's copyright policy will be subject to discipline by the District and may be subject to criminal or civil penalties.

Student users will not plagiarize materials. Teachers will instruct students in appropriate research and citation practices and will monitor and enforce such appropriate practices.

Software Installation

The technology staff shall perform all software installations. No student, employee or administrator shall install software on his/her personal or District computers using the Wissahickon Network Services ("WNS"). The Director of Technology shall maintain an updated license database to assure compliance and make budgetary decisions. Only software which is specifically approved by the Director of Technology and is owned by the District or subject to a license held by the District may be installed on the WNS or single client machines. Software purchased or otherwise acquired by employees, administrators and/or students shall not be installed on District computers or using the WNS unless the software is owned by and/or has been properly donated to the District and the original media is in the possession of the Director of Technology.

Establishment of Websites

1. District Website – The District shall establish and maintain a website and develop web pages that present appropriate information about the District. The Director of Technology will be responsible for managing and maintaining the District website.

2. School or Class Web Pages – District schools and classes may establish web pages that present information about the school or class activities. The building principal will designate an individual to be responsible for managing the school website under the supervision of the Director of Technology or his/her designee. Teachers will be responsible for maintaining all aspects of their class websites. The District reserves the right to prohibit or otherwise limit the content of any material contained on a website established by and/or existing through the WNS.

3. Extracurricular Organization Web Pages – With the approval of the Superintendent or his/her designee, extracurricular organizations may establish web pages. The Director of Technology will establish a process and criteria for the creation of such websites and posting of material, including linking to other sites, on these pages under the supervision of the building principal or his/her designee. Material presented on the organization web page must relate specifically to organization activities and will include only student-produced material. Organization web pages must include the following notice: "This is a student extracurricular organization web page. Opinions expressed on this page shall not be attributed to the Wissahickon School District or its Board Members, Administrators or Employees." The District reserves the right to prohibit or otherwise limit the content of any material contained on a website established by and/or existing through the WNS.

4. The District shall obtain written permission from both the parent/guardian and the student prior to placing any student photographs, artwork, writing, or other projects on a website. No personal contact information about a child, such as home address, phone number, or e-mail address will be included on a website using the WNS.

5. The inclusion of any student work will appear with a copyright notice prohibiting the copying of any protected student work without the required express written permission. All requests for written permission to copy any protected student work will be forwarded to the student's parent or guardian or to the student if age eighteen or older. All student work will be removed from the website at the end of the current school year.

User Responsibilities

1. Personal Safety

    a. Student users will not post personal contact information about themselves or other people. Personal contact information includes but is not limited to home address, telephone numbers,

school address, work address, e-mail addresses, dates of birth and social security numbers.

b. A student user will not meet with an adult he/she has met or otherwise communicated with online without their parent or legal guardian's prior approval and participation.

c. A student user will promptly report to his/her teacher or other school employee in regard to any e-mail or website content he/she receives that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

a. Student users will not attempt to gain unauthorized access to the WNS or to any other computer system through the WNS system, or go beyond their authorized access. This prohibition includes attempting to log in through another person's account or access another person's files, even if only for the purpose of "browsing."

b. Student users will not make deliberate attempts to disrupt the system performance or destroy data by introducing and/or disseminating a computer virus or by any other means.

c. Student users will not use the WNS to engage in any other illegal act, including but not limited to arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, or harassing and/or cyber-bullying of another person.

<u>System Security</u>

1. Student users are responsible for the use of their individual WNS account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.

2. Student users will immediately notify the building principal or other administrator if they have identified a possible security problem. Users may not search for security problems as this may constitute an illegal attempt to gain access.

3. Student users will avoid the intentional and/or inadvertent spread of computer viruses by following the District virus protection procedures. All diskettes and/or data transfer devices must be run through a virus check prior to use on any District system.

4. Student users will not introduce, remove or copy any application or operating system programs on or through WNS without prior approval from the Director of Technology.

5. No student user will connect or disconnect any device using WNS without prior approval from the Director of Technology.

Access to Inappropriate Material

1. Access to Inappropriate Material

   a. Student users will not use the District system to access material that is profane, obscene, pornographic, that advocates illegal acts, or that advocates violence or discrimination towards other people ("hate literature"). For students, a special exception may be made for "hate literature" if the purpose of such access is to conduct educational research and access is previously approved by both the teacher and the parent or legal guardian.

   b. If a user inadvertently accesses inappropriate material, he/she should immediately report the inadvertent access to their teacher in a manner specified by their school. This reporting will protect other users from accessing the same information, and the user against an allegation that he/she has intentionally violated the Student Acceptable Use Policy. The inappropriate material accessed shall not be provided to other users, as such action would constitute a violation of policy.

2. Commercial Purposes

   a. Student users will not use the District system for commercial purposes. Commercial purposes are defined as offering or providing, soliciting or requesting goods or services for personal use. District acquisition policies will apply to the District purchase of goods or services through the system.

3. Political Activities

   a. Student users will not use the District system for political lobbying. Students may use the system to communicate with their elected representatives to express their opinion on political issues.

Actions Resulting From Misuse

1. Deliberate and/or negligent abuse of WNS, the network, computing resource, or any other District resource could lead to disciplinary action. Any such action will be subject to applicable policies and procedures established by the District. Offenders may also be subject to criminal prosecution. Under existing Pennsylvania law, it is a felony punishable by fine up to $15,000.00 and imprisonment of up to seven (7) years for any person to access, alter, or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. Knowingly and without authorization, disclosing a password to a computer system, network, etc., is a misdemeanor punishable by a fine of up to $10,000.00 and imprisonment of up to five (5) years, as is intentional and unauthorized access to a computer, or alteration of computer software.