No. **826**

SECTION: OPERATIONS

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

Wissahickon School District
Ambler, Pennsylvania 19002

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

1. Purpose

The use of any and all information and telecommunications resources accessed through the Wissahickon Network Services ("WNS") will be in accordance with the law, in adherence with standards of the District and the community, and primarily for educational purposes consistent with the curricular goals of the District. Incidental personal use of network resources is permitted for employees so long as such use does not violate other applicable provisions of this policy and does not interfere with the systems operations or with other systems users, education, employment or WNS usage. Use of WNS for personal solicitation or profit is prohibited, unless prior written approval is given by the Superintendent or his/her designee.

2. Definitions

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

This policy is referred to as "Guest Acceptable Use Policy."

3. Guidelines

A. General

This policy and these guidelines shall apply to all guest users who obtain access privileges to or otherwise access networks and 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 appropriate, be applicable to the use of all District information and telecommunications resources, whether connected to an electronic network or operated on a "stand alone" basis, as well as access to information networks and services provided to the user by or through the District, regardless of the location or ownership or 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 network, will be provided to users solely for the purpose of aiding teaching, education and research.

The use of WNS is a privilege, not a right, which may be revoked by the Superintendent or his/her designee at any time for abusive conduct or violations of the conditions of the terms of this policy or the administrative guidelines in this policy. Such conduct may result in disciplinary action.

The WNS cannot warrant what functions of the system and network will meet any specific requirements, or that it will be error free or uninterrupted; nor shall it be liable for any direct, incidental, or consequential damages sustained or incurred in conjunction with the use, operation or inability to access or use the system or network, 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 computer viruses), which may be accessible or propagated through networks such as 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 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 corresponding or 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 public forum may be copied in subsequent communications, as long as proper reference is given to the original author of the copied information.

Guest users have no legitimate privacy expectation in the information or websites that they visit while using the WNS, as this information is stored on the network, which is the exclusive property of the District. The District may at any time without prior notice review any information on the District network.

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.

B. 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 indemnify the District against any damage incurred by the District caused by the use of the WNS in violation of this policy.

C. Due Process

The District will cooperate fully 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 an guest-user has violated the Guest Acceptable Use Policy, the guest-user will be provided with notice of the alleged violation and be given an opportunity to present an explanation in accordance with applicable law.

Disciplinary actions will address the specific concerns arising from the alleged violation of this policy.

All guest accounts through WNS may be revoked at the discretion of the Superintendent or his/her designee or the Director of Technology.

System users have no privacy expectation in the contents of their personal files and accessed information on the WNS.

Routine maintenance and monitoring of the system may lead to the discovery that user has or is violating the Guest Acceptable Use Policy, another District policy, the discipline 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 an guest user who has allegedly violated a District policy and/or the law.

D. Search and Seizure

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 right at all times to use a remote access feature which enables authorized District guests and other authorized individuals to view what appears on a user's monitor when the user is utilizing WNS.

E. 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 employee users.

District guest users are expected to comply with copyright law and the District's copyright policy. Any employee who violates 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.

F. Software Installation

The technology staff shall perform all software installations. No guest user 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 guests 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.

G. User Responsibilities

1. Network Security

    a. Guest users have different levels of WNS access and different levels of access than other users. It is imperative that guests do not let anyone else log on to their account or have access to their account while they are logged on.

    b. Guest users must keep their passwords secret and must not disclose them to anyone other than the Director of Technology, Network Administrator or System Administrator when required. The District reserves the right to change passwords every ninety (90) days or when otherwise needed to maintain network security.

    c. Guest users must log off or lock the system if they leave the room in which the computer from which they are they are logged on is located, if they will not be using the system for more than five minutes or if they will be unable to see and ensure that no one else is using the computer from which they are logged on.

2. Illegal activities

    a. Guest 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.

    b. Guest 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. Guest users will not use the WNS to engage in any other illegal act, including but not limited to arranging for the sale or the purchase of alcohol or illegal drugs, engaging in criminal activity, threatening the safety of a person or harassing another person.

H. System Security

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

2. Guest 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 as an illegal attempt to gain access.

3. Guest 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. Guest 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 guest user will connect or disconnect any device using WNS without prior approval from the Director of Technology.

I. Access to Inappropriate Material

1. Access to Inappropriate Material

    a. Guest 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 toward other people ("hate literature") unless such access is for research or educational purposes related to the guest's educational responsibilities.

    b. If a guest user inadvertently accesses inappropriate material, he/she should immediately disclose the inadvertent access to their principal or supervisor in a manner specified by the District. This reporting will protect other users from accessing the same information and the user against an allegation that he/she has intentionally violated the Guest 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. Guest 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. Guest users will not use the District system for political lobbying.

J. Actions Resulting From Misuse

Deliberate and/or negligent abuse of WNS, the network, computing resource, or any other District resource could lead to disciplinary action and revocation of usage privileges. Any such action will be subject to applicable policies and procedures established by the District and law.

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.