WARREN COUNTY SCHOOL DISTRICT	SECTION 9000

9900 MISCELLANEOUS INSTRUCTIONAL POLICIES

9950 Technology and Internet Safety

A. PURPOSE

Emerging software opportunities, electronic communication systems and networks (technology) allow for new methods of education and academic research in the District by providing resources and the opportunity for collaborative work. Telecommunications facilities, computer hardware and associated software opportunities, including educational computer programs, research via the World Wide Web, transfer of information and interaction with others via electronic mail, ~~news groups~~ **electronic collaboration tools,** and the like, should be utilized to support the District's curriculum and to support communications among the District's students and employees.

Although this technology allows significant opportunities for research, curriculum enhancement and improved communications, the technology also affords significant opportunities for abuse. This Policy is intended to establish guidelines for the appropriate usage of existing technology. Guidelines are also established for the introduction of new technology to be utilized in the educational setting.

Given the ever-changing nature of technology, its potential opportunities and abuses, it will not be possible for this Policy to address all specific situations, which may arise. Therefore, it is also the purpose of the Board, by this Policy, to vest in the Superintendent or his or her designee the authority to fashion procedures, as necessary, to implement the general purposes of this Policy.

B. DEFINITIONS

1. Minor – any student of school age.

2. Obscene - Analysis of the material meets the following elements:
   a. The average person applying contemporary community standards would find that the subject matter taken as a whole with respect to minors appeals to the prurient interest.
      1. Contemporary community standards shall be defined to mean the regions within which the District provides services to students.

   b. The subject matter depicts, describes or represents in a patently offensive way with respect to what is suitable for minors an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or a lewd exhibition of the genitals or post-pubescent female breast.

c. The subject matter taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

~~3. Contemporary community standards - The regions within which the District provides services to students.~~

3.~~4.~~ Harmful to minors - Any text, picture, image, graphic image file, or other visual depiction that:

a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion.

b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals.

c. taken as a whole lacks serious literary, artistic, political, educational, or scientific value as to minors.

4.~~5.~~ Child Pornography – any visual depiction, including any photograph, film, video, picture, or computer, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct, or (b) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

C. ACCESS **TO** TECHNOLOGY

Access to technology is provided to District employees and students as a privilege. Access is not and cannot be guaranteed. However, when access is available it is to be regarded as a privilege that carries with it a responsibility. All usage is to be done in a responsible, efficient and legal manner that is consistent with the values of the Student Discipline Code and the policies and mission of the District as enunciated in this Policy Manual or other directives of the Board or Administration. For users, the District's technology is to be used primarily for education-related purposes and performance of District job duties. Incidental personal use of school technology is permitted for employees so long as such use does not interfere with the District's Policy manual, the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy; procedures and rules contained in this policy, as well as Internet Service Providers, local, state and federal laws and must not damage the District's hardware, software, or technology. Students may only use the technology for educational purposes.

The District will notify the parents about the policies governing technology use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. **The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and Cyberbullying awareness and response.** 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 that parents bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District system.

D. GUIDELINES FOR USAGE

Usage of the technology~~,~~ which is not consistent with the "access" policy contained in the previous paragraph~~,~~ is prohibited. It is not possible to list all of the types of usage~~,~~ which are inappropriate. However, as a guideline, some of the types of inappropriate usage are listed below:

1. Engaging in non-work or non-school related communications unless for employees under this policy's definition of incidental personal use.

2. Sending or displaying of offensive messages or pictures, including but not limited to, messages or pictures that contain pornography, child pornography, matters that are obscene or matters that are harmful to minors, ethnic slurs, racial epithets, or anything that may be construed as disparagement of others based on their race, national origin, sex, sexual orientation, age, disability or religious or political beliefs.

3. Using obscene language.

4. Using technology to harass**,** threaten, disrupt, defame or annoy others.

5. Trespassing in or upon personal files or programs, removing, damaging or utilizing information which the user is not entitled to remove, damage or utilize or communicating under a false name or other false pretenses.

6. Violating any copyright laws or the Copyright Policy of the District including Policy Section 9905 by copying, downloading, uploading or otherwise duplicating copyrighted material.

7. Violating any other District Policy including policies concerning political activities and advertising such as Policy Number 7240.

8. Engaging in any use which violates any State or Federal law, rule or regulation.

9. Intentionally creating, uploading or other introduction of computer viruses or similar device or program, which damages hardware or software.

10. Engaging in unauthorized access of computers, intentionally disrupting the network or attempting to circumvent security measures on an individual computer and / or the District network.

11. Using the technology for gambling, sports pools, betting games or games of chance.

12. Installing, uninstalling or damaging computer hardware, software or the network.

13. Creating **such things as** documents, web pages, electronic communications, or videoconferences that include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

14. Unauthorized connection of non-district issued technology devices to the District network.

15. Creation of, or participation in, "chain letters" or similar forms of broadcast mail.

16. The use of profanity in any communication unless required for business purposes.

17. Using technology resources to access, inspect or disseminate confidential or personal information of others.

Any employee or student engaged in the inappropriate use of or access to the technology may be subject to the loss of the privilege. The Board hereby vests the Administration with the authority to restrict any person's usage of the privileges, for the period of time deemed appropriate by the Administration, on account of violations of this Policy. Additionally, students are advised that violations of this Policy may result in students being disciplined in accordance with the Discipline Code and employees are advised that violations of this Policy may result in discipline procedures according to the applicable sections of this Policy Manual or the Contract(s) governing the relationship between the District and employee.

E. FILTERING

The District uses a technology protection measure that is designed to prohibit users from accessing Network sites that are not in accordance with the policy and procedures of the District and the laws of Pennsylvania. This measure helps guard against access by users to messages or pictures that contain pornography, child pornography, matters that are obscene or matters that are harmful to minors, ethnic slurs, racial epithets, or anything that may be construed as disparagement of others based on their race, national origin, sex, sexual orientation, age, disability or religious or political beliefs. Filtering may be disabled for adults engaged in bona fide research or for other lawful purposes. To ensure enforcement of the policy, the District will monitor use of technology resources through direct supervision and monitoring of the network. This filtering measure is not foolproof and inadvertent access to sites not consistent with this policy needs to be reported immediately **to a District administrator.**

F. USER ACCOUNTS

All electronic communications initiated while utilizing the District technology shall be channeled through a User Account. User Accounts may be provided for District students and employees. Any student utilizing a User Account shall do so only with permission of a District employee. All User Accounts shall be the property of the District and shall be used only for the purposes described in this Policy. All User Accounts shall be accessed only via a password. Upon request, a student or employee shall make their password known to the Superintendent, the Technology Director, the Building Administrator or their designee. ~~No user may employ a password unknown to the District, and no~~ **No** user shall reveal their password to another individual except as set forth above or except as is absolutely necessary to carry out an educational objective. Except as is absolutely necessary to carry out an educational objective, no user is to utilize a computer that has been logged in under another individual's password.

G. SOFTWARE

Except as provided below, no software will be utilized on any computer or other component of the District's technology systems unless said software has been selected or approved by the Superintendent or his/her designee. The Superintendent will cause to be published a list of approved software, and any software referenced on said list may be utilized without obtaining other approval. District employees, students, or other persons desiring to see the introduction of software not approved by the above persons or referenced on the above list, shall make application for approval of the particular software according to procedure established by the Superintendent or his / her designee.

H. HARDWARE

It shall be the duty of all District employees to report ~~equipment~~ **technology** problems to the Building Administrator, and for the Building Administrator to report ~~equipment~~ **technology** problems to the Technology ~~Director~~ **Department**, or his /her designee through the ~~Technology Department~~ **District** Work Order system.

All computers or other technology system components belonging to the District are to remain in their designated areas. Prior to any change in equipment ~~Technology Department~~ **a District** Work Order must be completed and ~~signed by the Building Administrator and~~ submitted ~~to the Technology Director, or his /her designee,~~ for approval.

All purchases or acquisitions of computers or other components of the District's technology system, including donations of equipment from businesses, parent/teacher organizations and similar entities are to be channeled to the Building Administrator at the building at which the equipment is proposed to be installed. Before approving the installation of said equipment, the Building Administrator is to submit a description of the equipment to the Technology ~~Director~~ **Department**~~, or his/her designee,~~ for approval.

Building Administrators are expected to adopt appropriate procedures **to safeguard the investment of technology. As an example,** ~~in order to keep~~ food and drink ~~out of computer labs and away from computer systems and other technology system components.~~ **should not be permitted near computers or technology devices.**

I. REPAIRS

All repairs of the District technology system, including repairs to both hardware and software, and including in-house technician repairs and outside vendor services, are to be submitted on a Technology Department Work Order to the Building Administrator for approval. The Building Administrator shall forward all approved work orders to the Technology Director for his/her approval prior to the repair.

J. SEARCH, SEIZURE AND MONITORING

Users of the privileges should have NO EXPECTATION OF PRIVACY with regard to any information or communication on or exchanged through the District's technology. The District reserves the absolute and complete right to inspect and to seize any information or communication existing on any District technology equipment and any user of the said equipment must understand that the privilege is subject to the District's right of search and seizure. Any information or communication seized by the District may be used for any legitimate purpose, including usage in disciplinary proceedings initiated by the District and usage in criminal proceedings initiated by State or Federal officials to which the District has given the information or communication. The user of any District technology or software privilege is advised that the District, may

at any time, monitor persons' usage and that seizure of material may be made as a result of random searches and not necessarily as a result of reasonable suspicion or probable cause. ~~IF THE USER OF THE DISTRICT TECHNOLOGY DOES NOT WANT INFORMATION OR COMMUNICATIONS TO BE MADE PUBLIC, THE USER SHOULD NOT PLACE OR SHARE THAT INFORMATION OR COMMUNICATION ON THE DISTRICT'S FACILITIES~~ **If the user of the District technology does not want information or communications to be made public, the user should not place or share that information or communication on the District's facilities.** At all times the District reserves the right to:

1. Determine how its hardware space is utilized, including the right and ability to remove software, files, to compress or consolidate files, and to otherwise manipulate the data maintained on any computer or other component of the District's technology.

2. Restrict or limit usage of lower priority network and computer uses when network and computing requirements exceed available capacity.

3. Determine which technology will be provided through District resources.

4. View and monitor network traffic, file server space, processor and system utilization, and all applications provided through technology, including email

5. Log technology use by students and staff.

K. MISCELLANEOUS

1. Publishing on the Web. All Web pages to be created through the use of District technology shall be linked through the District Web Site. All District employees, students or school organizations wishing to create a Web page or similar device must create it under the supervision of the Superintendent, or his/her designee.

2. Limitation of Liability. The District makes no warranties of any kind, either express or implied, concerning the operation or the function of the privileges provided through the District's technology. All users of the District's privileges agree that the District will not be responsible for any damages users may suffer, including but not limited to loss of data or interruption of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for any financial obligations arising through the use of the privileges other than the provision of the hardware, software and utilities necessary to make the privileges available.

3. Curricular Usage of Telecommunications Devices. District employees may elect to utilize the technology system as a part of the instruction offered by that employee. In the event that a parent or legal guardian desires that their student not have access to the technology devices, the parent or guardian shall request an exemption in accordance with Section 9525 of this Policy Manual. In the event of an exemption, the District will provide an alternate means of instruction in accordance with Policy Section 9525

L. FUTURE DEVELOPMENTS

Technology devices and usage not currently contemplated will emerge. In recognition of the fact that particular provisions of this Policy may not be adequate to address those developments the Board hereby authorizes the Superintendent to develop procedure, on an as needed basis, to address emerging technologies or usage. In preparing these procedures, the Superintendent is directed to issue procedures which are consistent with this Policy and which are consistent with the values and mission of the District as enunciated in this Policy Manual or other directives of the Board. The procedures implemented by the Superintendent shall remain in effect until supplanted by the Board.

Revision Date	January 2004
Adoption Date-	March 8, 2004
Revision Date	
Practice	-
Legal Reference	-

AJS/lbc/rjf/kk