

**NETWORK USAGE AND SAFETY POLICY
ENCOMPASSING LOCAL, INTRANET AND INTERNET NETWORKS AND
RESOURCES UTILIZED BY
BOARD MEMBERS, STAFF, STUDENTS, PARENTS AND OTHER USERS
IN THE SCHOOL DISTRICT OF PITTSBURGH**

May 25, 2005

PURPOSE

This policy amends the former policy adopted on February 24, 1998 entitled **ACCEPTABLE USE OF THE INTERNET, INCLUDING LOCAL, INTRANET AND INTERNET COMPUTER NETWORKS FOR BOARD MEMBERS, STAFF, STUDENTS, AND OTHER USERS IN THE SCHOOL DISTRICT OF PITTSBURGH** in order to comply with the Children's Internet Protection Act (CIPA), and the Neighborhood Children's Internet Protection Act (NCIPA).

The Board supports use of Local, Intranet and Internet computer/resource networks in the School District's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the School District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students, and

The electronic information available to students and staff does not imply endorsement of the content by the School District nor does the School District guarantee the accuracy of information received on the Internet. The School District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The following procedures be followed with regard to the District's Local, Intranet and Internet computer/resource networks.

DEFINITIONS

1. **Acceptable Use**—utilizing District resources (network, computing devices or applications) to satisfy educational or administrative assignments, research or tasks described wholly as official PPS business in the context described in the Acceptable Use Policy.
2. **Access to Internet**—a computer shall be considered to have access to the Internet if such computer is equipped with a modem or is connected to a computer network which has access to the Internet.
3. **Authorized Account Owner**—an individual authorized by the District to have access to and utilize computers/networks and/or services owned, leased or operated by the District.
4. **Blog**—Short for Web Log; a web page that serves as a publicly accessible personal journal for an individual (Blogger). Typically updated daily, blogs often reflect the personality of the author.
5. **Child Pornography**—the term child pornography shall have the meaning given such term in section 2256 of Title 18, United States Code.
6. **Computers**—any and all computers, computer equipment, systems, hardware and/or software owned, leased or operated by the School District of Pittsburgh.
7. **Direct electronic communications**—any and all communications made or disseminated by electronic means, including but not limited to electronic mail, chat rooms or other forms of direct electronic communications.
8. **Fair Use Guidelines**—guidelines developed by the Working Group on Intellectual Property to clarify the application of fair use principles for educators considering digital copyright issues.
9. **Hacking**—the act of accessing or attempting to access targeted network resources, either internal or external, for the purpose of gathering/acquiring non-privileged access and/or information, passwords, functionality, identity theft or distribution of unsolicited scripts and/or viruses.
10. **Harmful to Minors**—any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors appeals to the prurient interest, depicts, describes or represents in a patently offensive way an actual or simulated sexual act or sexual conduct, as described by the Children's Internet Protection Act, and taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.
11. **Inappropriate matter**—In addition to items defined under "Harmful to Minors," any material that contributes to intimidation, constitutes a safety/security concern, threatens, is deemed as "tasteless" by the District's filtering application or violates any existing District Policy, including but not limited to Human Relations, Sexual Harassment and/or Student Code of Conduct.
12. **Inappropriate usage of District Computers/Internet/Hardware & Software Resources**—use of the District's computers and local, intranet and internet services,

owned, leased or operated, that violates the District's Policy on Internet Usage and Safety or conflicts with the District's mission and purpose or with an employee's authorized job duties or responsibilities. The school or office administrator shall have the authority to determine what is considered to be inappropriate use. Issues related to inappropriate use will be overseen by a steering committee.

13. **Individuals Covered by this Policy**—Board Members, Staff, Students, Parents and other Users of Computers/resource networks and/or services Owned, Leased or Operated by the School District of Pittsburgh.
14. **Instant Messaging**—Abbreviated *IM*, a type of service that enables users to communicate in real time over the Internet. Typically, the IM system alerts users whenever someone from their private list is online and a chat session can be initiated with that individual.
15. **Internet**—defined as the “standard” Internet (the collaboration and inter-connectivity of computer networks and resources worldwide) and Internet 2 (a higher educational/research form of non-commercial Internet access).
16. **Local, Intranet and Internet Computer Networks**—1.) Networks residing within the boundaries of a District-owned/leased facility. 2.) Leased/owned inter-connecting networks under the District's management. 3.) Outside, non-District owned/operated networks and corresponding resources.
17. **Minor**—an individual who has not attained the age of 17.
18. **Obscene**—the term obscene has the meaning given such term in section 1460 of Title 18, United States Code.
19. **Online**—active connection to network hardware, software or service resources.
20. **Rogue Access**—interpreted by the District as any connectivity to any District resources via internal network access (through devices, hard-wired drops or wireless) or external network access (Internet, Internet2, wireless, dial-in, VPN, or satellite) without explicit permission obtained through the District's Office of Information & Technology's Call Center.
21. **Rogue Devices or Applications**—hardware devices or software not authorized the Office of Information and Technology to be utilized on the District network infrastructure or computers.
22. **Sexual Act; Sexual Contact**—the terms sexual act and sexual contact have the meanings given such terms in section 2246 of Title 18, United States Code.
23. **Spam**—a slang term for e-mail that is the electronic equivalent of junk mail; usually advertisements, jokes or notices of no real value to the recipient.
24. **Technology Protection Measure**—specific technology that blocks or filters Internet access to visual depictions that are—a) obscene, as that term is defined in section 1460 of Title 18, United States Code; b) child pornography, as that term is defined in section 2256 of Title 18, United States Code; or c) harmful to minors.
25. **Vandalism**—any malicious attempt to harm or destroy the District's computers, data, applications, and/or network functionality or the data and/or functionality of another user's computer. This includes but is not limited to the uploading or creation of computer viruses.
26. **World Wide Web**—a collection of Internet sites that offer text and graphics and sound and animation resources through the hypertext transfer protocol. It is often abbreviated “WWW” or called “the Web.”

SAFETY PROCEDURES

All Internet access on District owned/leased resources will be filtered through the use of filtering software to prevent access by minors/parents/staff/outside users to inappropriate matter on the Internet and World Wide Web.

In order to restrict the access of minors/parents/staff/outside users to visual depictions that are obscene, child pornography, and other materials harmful to minors, filtering software will be utilized on all District computers with access to the Internet.

An administrator, supervisor, or other person authorized by the School District may request disabling a particular site from the filtering software, during use by an adult, in order to enable access for bona fide research or other lawful purpose. A custom request of this nature is initiated through the District's Call Center (412-390-2790) by the appropriate administrator, supervisor or authorized person. Upon receipt of a request the site will be reviewed for validity and access will be granted/denied accordingly.

Students will not be advised or encouraged by school staff to obtain free e-mail accounts through commercial providers (e.g., Hotmail, etc.) for use in class projects.

The District does not endorse or advocate the use of commercial Instant Messaging service and is not responsible for its content. Users shall not communicate electronically or agree to meet in person with unknown online acquaintances.

All individuals covered by this policy shall not participate in hacking or other unlawful online activities.

All individuals covered by this policy shall not while online disclose, use or disseminate personal identification information regarding minors or other users.

In a further attempt to ensure the safety and security of users, the online activities of users can/will be monitored and recorded.

USAGE PROCEDURES

Network accounts shall only be used only by the authorized owner of the account for its authorized purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

The content of the Information Security Policy is incorporated into these guidelines by reference.

Students, staff and other District resource users are expected to act in a responsible, ethical and legal manner in accordance with School District policy, accepted rules of network, usage and Federal and State and Local law.

The following types of usage are specifically prohibited and if performed will subject the user to certain consequences, including but not limited to loss of access and/or other disciplinary and/or legal actions:

1. Use of the network to facilitate any illegal activity including “hacking.”
2. Use of the network and/or its resources for commercial or for-profit purposes.
3. Use of the network and/or its resources for non-work or non-school related work.
4. Use of the network and/or its resources for product advertisement or political lobbying.
5. Use of the network and/or its resources for harassment, hate mail, discriminatory remarks, bullying and offensive or inflammatory communication.
6. Unauthorized or illegal installation, downloading, distribution, reproduction, or use of copyrighted materials, i.e., plagiarism.
7. Use of the network and/or its resources to access obscene, pornographic material, or other material harmful to minors.
8. Use of inappropriate language or profanity on the network and/or its resources.
9. Use of the network and/or its resources to transmit material likely to be offensive or objectionable to recipients, including but not limited to spam.
10. Use of the network and/or its resources to intentionally obtain or modify files, passwords, and data belonging to other users, internal or external to the District’s network.
11. Impersonation of another user, anonymity, and pseudonyms, i.e., identity theft.
12. Use of network facilities for fraudulent copying, communication or modification of materials in violation of copyright laws.
13. Copying, loading or use of unauthorized or pirated games, programs, files, data or other electronic media.
14. Use of the network and/or District resources to disrupt the work of other users.
15. Destruction, modification, vandalism or abuse of network hardware, software and/or functionality.
16. Quoting personal communications in a public forum without the original author’s prior consent.
17. The creation of links to other networks whose content or purpose would tend to violate these guidelines.
18. Attaching rogue devices or applications to District resources.
19. Sending unsolicited email for the purpose of advertisement or non-District business.
20. Installation and/or use of non-district authorized remote desktop or other computing utilities.

RESPONSIBILITIES

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or School District files. To protect the integrity of the system, the following guidelines shall be followed:

1. Only current staff, students, parents and approved outside users are authorized to have accounts on the network.
2. Employees, and students, parents and approved outside users shall not reveal their passwords to another individual.
3. Users are not to use a computer that is actively logged in under another user's name.
4. Any user identified as a security risk or having a history of problems with other computer systems, resources and/or networks may be denied access to the network.
5. No student shall ever be permitted to use/operate ANY staff computer for ANY reason.
6. All users must comply with the District's Password Policy.
7. All users must utilize the District's guidelines for Virus Protection, Information Security, Email Use, Internet and Web Site Development Safety.

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator. Correspondingly, the appropriate administrator should report the activity to the District's Call Center (412-390-2790).

Network users shall not reveal personal addresses, telephone numbers or any personal identification information about themselves or other users.

The illegal use of copyrighted software by users is prohibited. Any data uploaded to or downloaded from the network shall be subject to "fair use" guidelines.

The School District shall make every effort to ensure that this educational resource is used responsibly by students, parents, staff and approved outside users.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

All users have the responsibility to respect and protect the rights of every other user in the School District and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use. Issues related to inappropriate use shall be referred to the Acceptable Use Steering Committee for review.

ILLEGAL ACTIVITIES

Users shall not attempt to gain unauthorized access (hacking) to the District's network resources (equipment or applications) either internally through the District's network or an outside non-District network. This prohibition includes intentionally seeking information about passwords ("password cracking") belonging to other users, modifying passwords belonging to other users or attempting to log in through another person's account. Further, users may not attempt to access, copy or modify another user's files. These actions are not permitted and are illegal, even if only for the purposes of "browsing."

Users shall not go beyond their authorized access and permission level granted from the District.

Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by the Office of Information and Technology.

Users are also prohibited from destroying or vandalizing data, software or equipment.

Users shall not introduce or propagate computer viruses or worms.

Users shall not use any District resource to engage in any other illegal act.

CONSEQUENCES FOR INAPPROPRIATE USE

The network user shall be responsible for vandalism and/or other damages, including lost/extended resource time of Technology staff or outside contractors, affecting the equipment, systems, software and functionality resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion/manipulation or damage to files or data belonging to others; copyright violations or theft of services and/or identity will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using District computers, network hardware/software resources and/or the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary and/or legal actions shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.

FURTHER PROVISIONS

It should be noted that all District computers, leased or owned, are the property of the District and are to be utilized as a tool to assist in education and job duties. No right of personal usage extends to the end-user in regards to private property.

The Board establishes that use of the Internet is a privilege, not a right; and that inappropriate, unauthorized and/or illegal use will result in the cancellation of those privileges and appropriate disciplinary/legal action.

The School District reserves the right to log network use, to monitor fileserver space utilization by School District users, to restrict access to external network sites and to monitor e-mail usage, while respecting the privacy rights of School District users.

The School District shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

- a. The District shall not be responsible for restoring any personally installed applications or data deemed as having no educational value.
- b. The District reserves the right to re-image any District-owned/leased computer at its discretion.

The School District shall not be responsible for any unauthorized charges or fees resulting from a user's ability or inability to access the Internet.

This policy in no way affects the duties and/or responsibilities of a school district pursuant to the Family Educational Rights and Privacy Act (FERPA) and the PA Guidelines for Dissemination of Student Information, 22 Pa. Code §12.31 et seq.