

PITTSBURGH PUBLIC SCHOOLS
INFORMATION SECURITY POLICY

May 25, 2005

Purpose:

To provide guidelines which preserve the confidentiality of information in order to protect the right to privacy of individuals, the best interests of the Board, and enable each employee to carry out his or her responsibilities efficiently and effectively by insuring the accessibility and accuracy of information regarding students, personnel, school operation, business operation, and other aspects of the District's activities.

General Policy:

All employees having access to computers, computer resident information, or computer generated information within the context of their duties are required to be familiar with this policy. Additionally, this requirement applies equally to non employees granted access to such information in the context of performing services for or in the name of the District.

1. No person may, without appropriate authorization, access, copy, or modify in any way or manner, programs or files of information relating to students, staff, or District operations.
2. Enforcement of this policy is the responsibility of each school Principal or school site administrator, Office Director, and all employees bearing supervisory responsibility. In fulfilling this responsibility, it is expected that any necessary rules, directives, or procedures, will be established which are required or deemed appropriate in order to comply with the spirit of this information security and confidentiality policy.
3. Users who violate this policy will be subject to disciplinary action up to and including dismissal.
4. The District will participate in prosecution for violations of this policy to the extent allowed by law.
5. The Division of Communications & Marketing is responsible for periodically updating this policy as needed. Questions relating to this policy are to be directed to the Director of that unit.

Confidentiality of Information:

Information gained or available as a result of the performance of one's duties may not be discussed with, or revealed to, unauthorized individuals.

Users are granted access to a wide variety of information solely for the performance of routine tasks and assignments. It is important that each individual recognize the need to protect privacy rights of students and fellow employees and that unauthorized release of business related information could have a detrimental effect on the mission of the District. Each user should recognize his or her major role as an individual link in this privacy chain.

In some cases the confidentiality of information is protected by State or Federal law. Guidelines for the release of Information ultimately rest with the office and functional unit responsible for that information. Currently, general guidelines state that the Office of Human Resources be contacted regarding questions on staff information, Operations Office for business related data,

and the Office of Information & Technology regarding the release of student information. In some cases contact may be necessary with the Law Department. The Division of Communications & Marketing should be informed of any requests by media for information.

Computer User Responsibilities:

User-names and Passwords are to be kept confidential and passwords changed periodically.

Each computer user should understand that she/he has been given access to computers or computer information for a specific purpose and only that purpose. Computer and information access is controlled by a USER ID and PASSWORD assigned to that individual; anyone who has knowledge of a user-name and corresponding password is capable of doing the same operations on the computer as the individual to whom it was assigned.

All users are responsible for periodically changing their passwords in compliance with the District's posted *Password Policy*, to avoid compromising the security of the District's network.

Users are responsible for being familiar with the District *Information Security, Password Protection, Virus Protection, Internet Safety and Email Guidelines*.

Guidelines have been established to promote the use of appropriate practices which support the intent of this policy. These guidelines will be updated periodically as the need arises and will be posted in all offices so as to be accessible to anyone to whom this policy applies.

All critical data files must be periodically backed-up and stored either off-site or on-site in a container with a minimum fire rating of 1 hour UL Classified fire protection.

The District in whole creates daily backups of mission critical and personal data that are centrally stored. Each school or office maintaining locally stored (departmental server or workstation) data files critical to District operations is also responsible for creating a daily back-up copy of data, which can be used in the event of destruction or unavailability of the original.

Any known or suspected violations of this security policy must be reported to an immediate or appropriate supervisor.

Every employee has an interest in seeing that this policy is followed. Early detection of security problems will help minimize any damage which might occur. Employees who are aware of or suspect a security breach should immediately contact their direct supervisor or the District Call Center.

The District will participate in prosecution for violations of this policy to the full extent allowed by law.