Pennsbury School District
School Board Policy

Effective Date	Supercedes Index No.	Index No.
2/19/09	**NEW**	**830.1**

Title: Information Security and Confidentiality

Purpose: This procedure provides for compliance specifically with federal and state law and the Health Insurance Portability and Accountability Act (HIPAA), which requires entities to protect and secure personally identifiable health and financial information.

Definitions:

Access Control: The policies and procedures that control access to or provide authorized users with the ability or means necessary to read, write, modify, or communicate data or information or otherwise use any electronic information resource (EIR).

Authorized User: Any Pennsbury School District faculty, staff, or other individual affiliated with Pennsbury School District who has been granted authorization to access an electronic information resource or invokes or accesses an electronic information resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with Pennsbury School District. The authorization granted is for a specific level of access to the electronic information resource in accordance with the authorized user's job responsibilities.

Compromise: Unauthorized (actual or suspected) access, use, disclosure, modification, or destruction of an electronic information resource is a violation.

Electronic Information Resource (EIR): A resource used in support of Pennsbury School District activities that involve the electronic storage, processing, or transmitting of data as well as the data itself. Electronic information resources include application systems, operating systems, tools, communications systems, and data – in raw, summary, and interpreted form – and associated computer server, desktop, communications, and other hardware used in support of Pennsbury School District activities. Personally owned systems are included in this definition

if they connect to the Pennsbury School District network or are used to process or store Pennsbury School District information.

Public Information – Information accessible under the Public Records Act is available to any person notwithstanding their status or interest. Examples of public information include information made available to patient access via Pennsbury School District 's public web sites.

- **Restricted Data** – Information, which is not public information, but can be disclosed to or used by Pennsbury School District representatives to carry out their duties, providing there is no legal bar to disclosure.
- **Confidential Information** – Information that may or may not be protected by law but which is desired to be treated as confidential and protected accordingly. Access to confidential information is prohibited unless permitted by policy or exception to the law. In the case of legally confidential data, the exception may be contained within the law or regulation, or by court order or subpoena for the information.
- **Personal Information** – An individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security number; driver's license number; or an account, credit, or debit card number in combination with any required security code or password that would permit access to the account.
- **Protected Health Information (PHI)** – An individual's health information or data collected from an individual that is created or received by a health care provider, plan, or clearinghouse related to the past, present, or future physical or mental health or condition of the individual; the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual; identifies or could reasonably identify the individual; and is transmitted or maintained in electronic or any other form or medium.
- **Licensed Information** – Pennsbury School District members are obligated to insure that all copyright laws are flowed when using licensed information resources.

Security Incident

The attempted or successful unauthorized access, use, disclosure, compromise, modification, or destruction of an electronic information resource is a violation.

Security Threat: Any action by an individual or application that could result in a security incident that could compromise the confidentiality, integrity, or availability of data. Threats that could breach confidentially include, but are not limited to, unauthorized intrusions, malicious misuse, inadvertent compromise, viruses, or the loss or theft of a computing device that contains confidential or restricted information, or any incident in which a user either directly or by using a program performs functions for which they do not have authorization.

Information Technology Facilities: This policy applies to all computers and technology across the School District including but not limited to all associated networks, internet access, email, hardware, data storage, computer accounts, software, telephony services and voicemail.

Policy:

Access Control to the Information Technology Facilities: Authorized users of the information technology facilities must be aware of the conditions on which access is provided.

Access to the information technology facilities is restricted to authorized users. Access is normally based on job position and responsibility.

Login access to the information technology facilities shall be granted by the Director of Information Technology or his designee.

The Director of Information Technology or designee may restrict access to an individual user on the grounds that the user is in breach of this acceptable use policy.

The School District will not defend or support any member who uses information technology facilities for an unlawful purpose.

Unlawful use will breach this policy and will be dealt with as a discipline offence. Unlawful use of information technology facilities may also lead to criminal or civil legal action being taken against individual students or employees. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment.

Responsibilities of users: Each user is responsible for

- The unique user accounts which the School District has authorized for the user's benefit;
- Selecting and keeping a secure password for each of these accounts;
- Not sharing passwords and logging off after using a computer;
- Not compromising or attempting to compromise the security of any information technology facility belonging to Pennsbury School District or other organizations or individuals, nor exploit or attempt to exploit any security deficiency;
- Using the Information Technology facilities in an ethical and lawful way, in accordance with all federal, state, local laws.

Misuse of Information Technology Facilities: Users are

- Expressly forbidden unauthorized access to accounts, data or files;
- Not permitted to use School District information technology facilities for unlawful activity, e.g. infringement of copyright, defamation, etc;

- Use of electronic resources provided by the School District is governed by individual license agreements and is for non-commercial use only;
- Required to comply with use restrictions set out on the specific site or stated in the license agreement, and must not systematically download, distribute or retain substantial portions of information;
- Not permitted to utilize the School District's Information Technology facilities to access pornographic material or to create, store or distribute pornographic material;
- Not allowed to play electronic games on School District information technology facilities;
- Not permitted to use School District information technology facilities to sell or purchase any goods;
- Not permitted to run a business or to publish a journal or magazine on School District information technology facilities.

Confidentiality, integrity, and availability shall be protected for restricted or confidential information, including personal information and protected health information (PHI), when such information is created, received, transmitted, and/or stored in any medium, including electronic or paper format, and will ensure that the handling of such information is consistent with federal, state and local laws and policies.

Each user is responsible for the security and protection of electronic information resources over which he or she has control.

The School District reserves the right to withdraw a service or withdraw access if there is evidence of misuse of information technology facilities.

Responsible Administrator: Director, Information Technology