HAVERHILL PUBLIC SCHOOLS

WRITTEN INFORMATION SECURITY PROGRAM

I. OBJECTIVE

The objective of Haverhill Public Schools ("HPS") in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of Personally Identifiable Information ("PII"). The WISP sets forth HPS' procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII. **This WISP does not replace or supersede any of HPS' existing or future policies or procedures with respect to the safeguarding and/or handling of student education records data protected under the Family Educational Rights and Privacy Act (FERPA).**

For purposes of this WISP, "PII" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual:

- Social Security number;
- Driver's license number or government-issued identification number;
- Tribal identification card;
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account;
- Passwords, personal identification numbers, or other access codes;
- Any other numbers or information that can be used to access a person's financial resources;
- Digital signatures;
- Passport number;
- Student number;
- Date of birth;
- A birth or marriage certificate;
- The maiden name of the individual's mother;
- A private key that is unique to an individual and that is used to authenticate or sign an electronic record;
- An individual's taxpayer identification number or an identity protection personal identification number issued by the IRS;
- Medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or health insurance information;
- Biometric data, including fingerprints;
- DNA profile;
- Health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify an individual, or any information in an individual's application and claims history, including any appeals records;

- Username or email address coupled with a password or security question and answer that would permit access to an online account;
- Information or data collected through the use or operation of an automated license plate recognition system (a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data);
- Shared secrets or security tokens that are known to be used for data based authentication;

It also includes the following regardless of whether it is combination with an individual's first and last name or first initial and last name:

- Username or email address coupled with a password or security question and answer that would permit access to an online account;
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to that account;
- Any of the above data elements if the information compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

"PII" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

The purpose of the WISP is to better:

- Ensure the security and confidentiality of PII;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In formulating and implementing the WISP, HPS has addressed and incorporated the following protocols:

(1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII;

(2) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII;

(3) evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;

(4) designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of the regulations; and

(5) implemented regular monitoring of the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR

HPS has designated Douglas Russell (Director of Technology) to implement, supervise and maintain the WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Initial implementation of the WISP;

b. Training employees;

c. Regular testing of the WISP's safeguards;

d. Evaluating the ability of each of HPS' third party service providers to implement and maintain appropriate security measures for the PII to which HPS has permitted them access, consistent with the regulations; and requiring such third party service providers by contract to implement and maintain appropriate security measures;

e. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in HPS' practices that may implicate the security or integrity of records containing PII; and

f. Conducting training sessions for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to PII on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with HPS' requirements for ensuring the protection of PII.

V. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

Internal Threats

- HPS shall only collect PII of clients, investors, customers, suppliers, vendors or employees that is necessary to accomplish HPS' legitimate need to access said records, and for a legitimate job-related purpose, or necessary to HPS to comply with state or federal regulations.

- Access to records containing PII shall be limited to those persons who are reasonably required to know such information in order to accomplish HPS' legitimate business/educational purpose or to enable HPS to comply with state or federal regulations.

- Access to PII shall be restricted to active users and active user accounts only.

- Any PII stored shall be disposed of when no longer needed for business/educational purposes or required by law for storage. Paper or electronic records (including records stored on hard drives or other electronic media) containing PII shall be disposed of only in a manner that complies with the regulations and as follows:

    - Paper documents containing PII shall be either redacted, burned, pulverized or shredded upon disposal so that PII cannot be practicably read or reconstructed; and

    - Electronic media and other non-paper media containing PII shall be destroyed or erased upon disposal so that PII cannot be practicably read or reconstructed.

- A copy of this WISP must be distributed to each current HPS employee with access to PII and to each new HPS employee with access to PII at the commencement of their employment.

- All HPS employees with access to PII shall participate in HPS' training program on the detailed provisions of the WISP. All HPS employees with access to PII shall also participate in cybersecurity trainings hosted by HPS's Technology Department in partnership with the State of Massachusetts and our District Leadership, as well as participate in the review of regularly-generated cybersecurity "newsletters" that are prepared and circulated by the HPS Technology Department. Immediate retraining of HPS employees shall occur to the extent the Data Security Coordinator determines a need.

- <u>Procedures for Terminated Employees</u> (whether voluntary or involuntary)

    - Terminated employees must return all records containing PII, in any form, which may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)

- A terminated employee's physical and electronic access to PII must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

- All persons who fail to comply with this WISP shall be subject to disciplinary measures, irrespective of whether PII was actually accessed or used without authorization.

- All security measures shall be reviewed at least annually, or whenever there is a material change in HPS' organizational practices that may reasonably implicate the security or integrity of records containing PII. The Data Security Coordinator shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

- <u>Physical Assets Protocol</u>

  - All assets must be secured from theft by locking up and maintaining a secure workplace, whether that work takes place in HPS' offices, client site, a car, hotel or a home.

    - All laptops must be placed in the trunk of vehicle when and wherever they are parked. If no secure trunk or other storage is available, employees must keep their laptops in their possession.
    - Laptops, PDAs, and other portable devices left in the office or at home over night should be kept in a locked and secure location.
    - Employees must have assets secured or within their physical possession while on public or private transportation, including air travel.
    - An employee's failure to adhere to this and other security policies of HPS may result in disciplinary action and, in case of preventable loss or theft, employee's replacing all assigned equipment at their own expense.
    - PII should not be stored on the local drive; it should be stored on the HPS network.

- <u>Access Control Protocol</u>

  - Access to electronically stored PII shall be electronically limited to those HPS employees having a unique log-in ID.

  - Employees must ensure that all computer systems under their control are locked when leaving their respective workspaces. Employees must not disable any logon access.

- Employees must log off the HPS network when they are not directly using those resources.

- All computers that have been inactive for 30 or more minutes shall require re-log-in.

- After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator.

- Employees must maintain the confidentiality of passwords and access controls:

    - All passwords used for HPS systems and laptops are required to adhere to strong password rules.
    - All passwords used for HPS systems and laptops are required to be changed every 6 months.
    - Employees must not share accounts or passwords with anyone.
    - Employees must not record passwords on paper or in a document.

- Where practical, all visitors who are expected to access areas other than common retail space or are granted access to office space containing PII should be required to sign-in at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.

- Where practical, all visitors are restricted from areas where files containing PII are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing PII are stored.

- HPS employees are required to report suspicious or unauthorized use of PII to the Data Security Coordinator immediately.

- Pursuant to HPS' Incident Response Plan, whenever there is an incident that requires notification under any state breach notification statute or regulation, there shall be an immediate mandatory post-incident review of events and action taken, if any, with a view to determining whether any changes in HPS' security practices are required to improve the security of PII for which HPS is responsible.

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

External Threats

- Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes PII.

- All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes PII.

- To the extent technically feasible, all PII stored on laptops or other portable devices shall be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

- There shall be secure user authentication protocols in place that:

    - Control user ID and other identifiers;

    - Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;

    - Control passwords to ensure that password information is secure.

- PII shall not be removed from HPS's premises in electronic or written form absent a legitimate need and use of reasonable security measures, as described in this WISP.

- All computer systems shall be monitored for unauthorized use or access to PII.

VII. CONTACT IN CASE OF LOSS/THEFT OR SUSPECTED LOSS/THEFT

If you have reason to believe that any PII has been lost or stolen or *may* have been compromised or there is the potential for identity theft, regardless of the media or method, report the incident immediately by submitting a ticket at http://support.haverhill-ps.org/ during normal working hours and 978-420-1980 after hours to report the incident.