Natick Public Schools
Written Information Security Policy
for Faculty, Staff, and Elected Officials/Committee Appointments

I. OBJECTIVE:

The objective of the Natick Public Schools in the development and implementation of this comprehensive Written Information Security Policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information of our students and our staff.

II. PURPOSE:

The purpose of the WISP is to better: (a) ensure the security and confidentiality of personal information; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) 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, the Natick Public Schools 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 personal information;

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

(3) evaluated the sufficiency of existing policies, procedures, 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 compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H; and

(5) implemented regular monitoring of the effectiveness of those safeguards. 1132900v1

IV. DATA PRIVACY TEAM:

The Natick Public Schools has established a Data Privacy Team to implement, supervise and maintain the WISP.

Our Data Privacy Team acts as stewards in all data privacy and protection decisions and consists of the following positions:

Superintendent
Assistant Superintendent of Teaching, Learning & Innovation
Assistant Superintendent of Student Services
Director of Technology
Director of Digital Learning
Director of Finance
Director of Human Resources
Director of Communications

Emailing dataprivacy@natickps.org will send a message to the entire Data Privacy Team. Please do so with any questions, concerns, complaints, or to report a data privacy or security issue. Any disputes concerning the processing of the PII will be responded to within three (3) weeks.

All updates regarding data privacy and security are located on our website at http://www.natickps.org/about/data_privacy

This team will be responsible for the following:

- Implementation of the WISP including all provisions outlined in Section VII: Daily Operational Protocol;
- Training of all employees;
- Regular testing of the WISP's safeguards;
- Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures;
- Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our school or district practices that may implicate the security or integrity of records containing personal information;

- Conducting an annual training session for all faculty, long and short term subs, coaches, administrators, staff, including temporary and contract employees, and elected officials/committee appointees who have access to personal information 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 our requirements for ensuring the protection of personal information.

V. INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, 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:

- We will only collect personal information of students or employees that is necessary to accomplish our legitimate school or district business or to comply with any and all federal, state or local regulations.

- Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.

- Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with school or district needs or legal retention requirements and with notice provided to parents/legal guardians and/or students in accordance with state law.

- A copy of the WISP will be distributed electronically to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging, and electronically signing, that he/she has received a copy of the WISP and will abide by its provisions. Employees are encouraged and invited to advise the Data Privacy Team of any activities or operations which appear to pose risks to the security of personal information. If any member of the Data Privacy Team is involved with these risks, employees are encouraged and invited to advise any other school or district leaders.

- Mandatory annual training for all current employees will be held at the start of each school year to detail the provisions of the WISP.

- All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP.

- Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee.

- A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All computer equipment, keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.

- Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.

- All security measures including the WISP shall be reviewed at least annually to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.

- Should our school or district practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.

- The Data Privacy Team shall be responsible for all review and modifications of the WISP and shall fully consult and apprise the School Committee of all reviews including any recommendations that improves security arising from the review.

- All building principals or his/her designee shall maintain a secured and confidential master list of all lock combinations, codes, and keys. The list will identify which employees possess keys, keycards, or other access devices and that only approved employees have been provided access credentials.

- The Data Privacy Team shall ensure that access to personal information is restricted to approved and active user accounts.

- Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, more often as needed. Employees should not use the same passwords for school accounts as for personal accounts. Any user suspecting that his/her password may have been compromised must report the incident to their supervisor and change all passwords immediately. Users should not disclose their passwords to anyone as stated in RUP.

- All employees are required to enable multi factor authentication (MFA) in order to be provided access to a school network account or school resources. Employees may use a cell phone to do this or request a security key if a cell phone is not available.

- Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Privacy Team.

- Whenever there is an incident that requires notification pursuant to the Security Breach Notifications of Massachusetts General Law Chapter 93H: "Security Breaches", the Data Privacy Team shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information.

VI. EXTERNAL RISK MITIGATION POLICIES:

- 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 personal information.

- Personal information shall not be removed from school or district premises in electronic or written form absent legitimate school or district need and use of reasonable security measures, as described in this policy.

- 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 personal information.

- There shall be secure user authentication protocols in place that:
    - Controls 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.
    - Enable and maintain multi factor authentication (MFA) to ensure secure access to all school accounts and resources.

VII. DAILY OPERATIONAL PROTOCOL

This section of our WISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our students and/or employees.

The Daily Operational Protocol shall be reviewed and modified as deemed necessary at a meeting of the Data Privacy Team and personnel responsible and/or authorized for the security of personal information. Any modifications to the Daily Operational Protocol shall be published in an updated version of the WISP. At the time of publication, a copy of the WISP shall be distributed to all current employees and to new hires on their date of employment.

A. Recordkeeping Protocol: We will only collect personal information of students and employees that is necessary to accomplish our legitimate school or district business or to comply with any and all federal and state and local laws.

- Any personal information stored shall be disposed of when no longer needed for school or district purposes or required by law for storage and pursuant to disposal notice requirements under federal and state law. Disposal methods must be consistent with those prescribed by the WISP.

- Any paper files containing personal information of students or employees shall be stored in a locked filing cabinet. Only building leaders, district leaders, department heads or employees that require access to do their primary job function will be assigned keys to filing cabinets and only those individuals are allowed access to the paper files. Individual files may be assigned to employees on an as-needed basis by the department supervisor.

- All employees are prohibited from keeping unsecured paper files containing personal information in their work area when they are not present (e.g. lunch breaks).

- At the end of the work day, all files containing personal information are to be returned to the locked filing cabinet.

- Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with M.G.L. c. 93I sec. 2 and as follows:

  (a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

  (b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

- Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as is and where transmitted. If encryption software is needed, please contact our technology services help desk at X5555 for assistance.

- If necessary for the functioning of individual departments, the department head, in consultation with the Data Privacy Team, may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP.

B. Access Control Protocol:

- All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the school district.

- Any employee leaving sight of their computer while it is on must lock it requiring a password to regain access, or configure their computer to automatically lock after 5 minutes of inactivity and require re-log-in.

- Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique log-in ID assigned by the Data Privacy Team.

- Where practical, all visitors (including all third party vendors) who are expected to access areas other than public spaces such as information technology closets or computer rooms, or granted access to office space that may contain personal information should be required to sign-in with a Photo ID 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 personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.

- Cleaning personnel (or others on site after normal school hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored.

- All computers with an internet connections or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

- An inventory of all school or district computer devices authorized for local personal information storage is contained in district technology inventory system, which shall be made known only to the Data Privacy Team and other managers on a "need to know" basis.

- The District will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.

C. Third Party Service Provider Protocol: Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information ("Third Party Service Provider") shall be required to sign a Data Privacy Agreement ("DPA") prior to providing the service. (Examples include third parties who provide off-site backup storage copies of all our electronic data; paper record copying or storage service providers; contractors or vendors working with our students or employees and having authorized access to our records):

- It shall be the responsibility of the Data Privacy Team to obtain reasonable confirmation that any Third Party Service Provider is capable of meeting security standards consistent with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H.

- If a vendor will not sign the DPA, the District will seek parent/guardian consent for the information to be shared with a vendor and provide the vendor's privacy policy to the parents/guardians.

VIII. Breach of Data Security Protocol: Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

- Employees are to notify the Data Privacy Team or department head in the event of a known or suspected security breach or unauthorized use of personal information.

- The Data Privacy Team shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office, to the extent there is a "data breach." A "data breach" is the unauthorized acquisition or use of sensitive personal information that creates a substantial risk of identity theft or fraud. Sensitive personal information is " resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

    - Social Security number;
    - driver's license number or state-issued identification card number; or
    - 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 a resident's financial account.

- The security breach notification for a "data breach," shall include the following:

    - A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    - The number of Massachusetts residents affected at the time the notification is submitted;
    - The steps already taken relative to the incident;
    - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    - Information regarding whether law enforcement officials are engaged in investing the incident.

- In the case of a "data breach", the Data Privacy Team will notify affected individuals about:

    - Consumer's right to obtain a police report
    - Information on how to request a security freeze at no charge
    - Information needed to request a security freeze
    - Information on complimentary credit monitoring services.
    - Name of the parent organization and subsidiary organizations affected