Natick Public Schools
Student Data Privacy Policy

I. OBJECTIVE:

The objective of the Natick Public Schools in the development and implementation of this Data Privacy Policy ("DPP"), is to be transparent with the community about the information we collect, how we use information, how we share information, how we protect information, how to contact us with questions, concerns or to report potential violations, and to comply with our obligations under all federal, state and local laws.

II. PURPOSE:

The purpose of the DPP is to better: (a) understand what is "personally identifiable information" ("PII"), and the laws and requirements that govern its protection; (b) be aware of the types of data we collect, how we use it, and when not to use it; (c) understanding third parties are required to be fully vetted by the school district before given access to any student data; (d) and establish a process for asking questions or reporting any violations of this policy.

For purposes of this DPP, "personally identifiable information" ("PII") for students is defined as any information that is not directly listed as directory information and whereby a "reasonable person in the school community" who does not have personal knowledge of the relevant circumstances could identify the student. It includes direct identifiers (such as a student's or other family member's name, or student id number) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). It includes all information, including recording and computer tapes, microfilm, microfiche, or any other materials regardless of physical form or characteristics concerning a student that is organized on the basis of the student's name or in a way that such student may be individually identified,

Protecting students' PII is to comply with our obligations under the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq. and several Massachusetts student privacy laws, including Massachusetts student record regulations, 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00.

III. INFORMATION WE COLLECT:

We collect various types of information provided by families of students, including, but not limited to:

Information Required for Student Enrollment

We collect various personal information for each student that enrolls in the Natick Public Schools.

This information includes but is not limited to:

- Biographical Information
- Parent/Legal Guardian Information
- Custodial Agreements
- Previous School Information (if any)
- Demographic Information
- Health & Medical Information
- Family Financial Information - if applying for financial assistance

Information Created once a Student is Enrolled in School

- Student ID Number
- Student Email Address
- Assessments, Grades / Transcripts
- Attendance Records
- Discipline Records
- Student Schedules
- Exams, Papers, Assignments, etc.
- Advising Records
- Individual Education Plans ("IEP") & 504s
- Transportation Information
- Bank or Credit Card Information - POS or to pay any fees

Other Information that is Collected

Student Web Searches: A content filter is in place on the school network that tracks and blocks a student's attempts to access inappropriate content and websites visited. The content filter overwrites this information every 7 days.

Student Email: All student email, using their school-issued email address, is archived. This

information is collected in the event it is needed to investigate a student conduct issue or Student related concern. All investigations follow a protocol of approval or if required by local or federal laws. Archived information is purged annually, over the summer, for students no longer enrolled in the district.

Video Surveillance: This is used in or around a school to ensure a safe environment for our students, faculty & staff and to aid in any investigation or incident reported at a school. Video footage is retained for up to 30 days then overwritten unless preserved for any current investigation or incident.

Tracking of School-Owned Devices: All school-owned devices have location tracking enabled so the device can be found if reported lost or stolen, needs to be audited, or requires a Software update to perform at the level needed. Location is limited to the last known location.

IV. HOW WE USE INFORMATION

We use the information provided by families and the data students create to provide the best possible educational opportunities for all of our students. This may include:

- Providing personalized educational services to help students achieve greater learning outcomes.
- Communicating with you, which may be to respond to inquiries or events happening at school.
- Providing you with information, including communications of interest based on email lists, text lists, or other electronic communications you joined.
- Improving, delivering, maintaining and protecting the learning environment we have created for our students, faculty & staff.
- Ensuring the safety, security, and integrity of all of our schools and the educational services we provide.
- Family financial information may be collected and used to determine the eligibility of local, state or federal financial assistance programs.
- Bank or credit card information may be collected by third-party vendors we partner with to provide school lunches or processing payment of fees.

V. HOW WE SHARE INFORMATION

We share PII with school administrators, teachers, counselors and other professionals who are employed by the school committee or who are providing services to the student under an agreement with the school district, and who are working directly with the student in an administrative, teaching counseling, and/or diagnostic capacity. Any such personnel who are not employed directly by the school committee shall have access only to the student record information that is required for them to perform their duties.

We share PII with administrative office staff and clerical personnel, including operators of data processing, who are either employed by the district or are employed under a service contract, and whose duties require them to have access to student records for purposes of processing information for the student record.

We work with third-party vendors to deliver many of our educational programs and services that support our schools. We require all vendors that store, manage or have access to our student information to sign a Data Privacy Agreement ("DPA"). 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. The goal of this DPA is to ensure all third parties:

- Follow all local and federal laws protecting students' rights for data privacy - FERPA, CIPA, COPPA, and PPRA and state law.
- Ensure the school district retains ownership of all student data regardless of where the data resides.
- Provide the school district notification of a data breach, if one should occur, within a specific time frame.
- Not resell or use student information for any other purpose than the service it was intended.
- Provide the school district the right to audit the vendor for compliance.
- Ensure industry best practices are being followed with respect to data privacy and data security.

VI. HOW WE PROTECT INFORMATION

The Natick Public Schools takes data privacy very seriously. Ensuring student data is protected is not a one-time event but part of our ongoing efforts of implementing best practices throughout the district.

Data privacy, however, isn't possible without having the proper controls in place to ensure data security, along with raising awareness among with all faculty, staff, students, parents, vendors, and members of the community we serve. Below are steps the district has taken to ensure both data privacy and data security so students' private information remains protected:

- The Natick Public Schools transitioned from Acceptance Use Policies to Responsible Use Policies for our students, faculty, and staff. In these policies are specifics guidelines for digital citizenship, data privacy, and data security.

- Natick Public Schools has been working with the Massachusetts Student Privacy Alliance ("MSPA"), The Education Cooperative ("TEC"), and our legal counsel to develop a standardized DPA for all vendors that store any student information with PII. TEC represents a number of school districts across Massachusetts concerned with student data privacy. Utilizing TEC's partnership with other school districts puts us in a stronger position when negotiating contract terms than going it alone and sends vendors a strong message that data privacy is an important issue we need to work on together to solve.

    - View a current list of executed vendor DPAs.

- The Natick Public Schools has implemented an internal vetting process, so all new vendors get on-boarded only after a data privacy agreement is agreed to and fully executed. 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.

- The Natick Public Schools has a "Written Information Security Policy" ("WISP") and has adopted and conducted a self-assessment of the Critical Security Control framework developed by the Center for Internet Security. These are ongoing efforts to ensure the implementation of best practices within all of our schools regarding data security.

- The school district is also implementing COSN's Trusted Learning Environment framework. This framework gets students, teachers, administrators and the entire community involved in our data privacy and data security initiative. The goal is not to earn COSN's seal of approval, but to raise awareness of the ongoing need for data privacy and data security, and change our behavior so data privacy and data security are a consideration in everything we do.

VII. DATA PRIVACY TEAM

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