

NORMAN HOWARD SCHOOL DATA SECURITY AND PRIVACY POLICY

The Norman Howard School is committed to maintaining the privacy and security of student data and teacher and school leader data and will follow all applicable laws and regulations for the handling and storage of this data and when disclosing or releasing Personally Identifiable Information (“PII”) to others. The School adopts this policy to implement the requirements of Education Law § 2-d and its implementing regulations.

Parent and Student Rights Under State and Federal Law

This policy shall include all protections given to parents/persons in parental relationship and students pursuant all State and federal laws that protect student data, including but not limited to School policies implementing the Family Educational Rights in Privacy Act and the Americans with Disabilities Act.

Parents Bill of Rights

1. A student’s personally identifiable information (PII) cannot be sold or released for any commercial purposes.
2. The School assures that the confidentiality of electronically stored PII is protected using safeguards that comport with industry standards and best practices, including but not limited to, encryption, secure firewalls, and password protection when student data is stored or transferred.
3. Parents have a right to inspect and review the complete contents of the student’s educational record, including portions of the record that are stored electronically, even when the record is maintained by a third-party contractor.
4. Parents have a right to review a complete list of all student data elements collected by the New York State Education Department (“NYSED”), published on NYSED’s website at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>. Parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to file written complaints with the School about possible privacy breaches of student data by the School’s third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to the School may be submitted to the School’s Data Protection Officer, Renee Widor, and can be submitted via email at rwidor@normanhoward.org or by mail at Renee Widor, Data Protection Officer, The Norman Howard School, 275 Pinnacle Road, Rochester, New York 14623.

6. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, emailed to CPO@mail.nysed.gov.

The School shall publish this Parent Bill of Rights in an appropriate location on the School's website.

Use and Disclosure of Personally Identifiable Data

As part of its commitment to maintaining the privacy and security of student data and teacher and school leader data, the School will take steps to minimize its collection, processing, and transmission of PII. Every use and disclosure of PII by the School shall be for the purpose of benefitting students and the School (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations), or to comply with State or Federal mandates (e.g., reporting requirements).

No personally identifiable information may be included in public reports or other documents, unless otherwise authorized by law.

Nothing in Education Law § 2-d or this policy should be construed as limiting the administrative use of student data or teacher or school leader data by a person acting exclusively in the person's capacity as an employee of the School.

NYSED Chief Privacy Officer

The School will comply with its obligation to report breaches or unauthorized releases of student data or teacher or school leader data to the NYSED Chief Privacy Officer in accordance with Education Law.

Data Protection Officer

The School shall designate a Data Protection Officer who shall be an employee of the School and responsible for the implementation and oversight of this policy and any related School procedures including those required by Education Law § 2-d and its implementing regulations. The Data Protection Officer will also serve as the main point of contact for data privacy and security for the School.

The Chief Executive Officer shall ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

Reporting a Breach or Unauthorized Release

The School shall develop written procedures for complaints to the School in accordance with Education Law 2-d and implementing regulations 8 NYCRR 121.4. The procedures shall be posted on the School's website along with this Policy.

The Chief Executive Officer or designee will report every discovery or report of a breach or unauthorized release of student data or teacher or school leader to the NYSED Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

School Data Privacy and Security Standards

The School will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) ("Framework") as the standard for its data privacy and security program.

Third-Party Contractors

Any and all contracts between the School and third-party contractors, under which a contractor will receive student data or teacher or school leader PII, shall include provisions requiring that the contractor and any sub-contractors maintain the confidentiality of shared student data or teacher or school leader data in accordance with law, regulation, and this policy.

In addition, the School will ensure that the contract or written agreement includes a signed copy of the Parents Bill of Rights and the contractor's data privacy and security plan, in compliance with Part 121 of the Commissioner's regulations and that has been accepted by the School.

The School will publish on its website a supplement to the Parents Bill of Rights for any contract or other written agreement it has entered with a third-party contractor that will receive PII from the School. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the School's data and/or technology infrastructure.

Agreements subject to this policy include any written agreements, agreements created in electronic form and signed with an electronic or digital signature, or a click wrap agreement that is used with software licenses and downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

Annual Data Privacy and Security Training

The Chief Executive Officer or designee shall ensure that annual data privacy and security awareness training is provided the School's officers and staff with access to PII. This training will

include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. This training may be delivered using online training tools. Additionally, this training may be included as part of the training that the School already offers to its workforce.

Notification of Policy

This policy will be published on the School's website and a copy shall be given to all officers and staff of the School.