

NORTHERN ADIRONDACK CENTRAL SCHOOL DISTRICT DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Supplemental Information Regarding Third Party Contractors
Parents' Bill of Rights
Data Security and Privacy Policy

This Agreement is between
Northern Adirondack Central School District and
[Great Minds] beginning on [09/01/2024] and ending on [08/31/2027]
PBC

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Northern Adirondack Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher/principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with the Bill of Rights:

- 1.) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract:

Great Minds will use student and staff PII only to provide contracted services to the School District. Aggregate, anonymized, and de-identified data are not student records nor Personally Identifiable Information and may be used by Great Minds for its business, commercial, marketing and research purposes.

- 2.) How the third-party contractor will ensure that the subcontractors, or authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data with, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g. FERPA; educational Law 2-d):

Great Minds employees and subcontractors are legally obligated to keep customers' personal information confidential and are provided only with the information that they need to perform their specific function. Additionally, subcontractors are required to maintain reasonable security practices, to use the information only for the purpose that we prescribe, and to prevent disclosure of the information to unauthorized parties.

- 3.) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g. whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed):

The contract expires on 8/31/2027. Upon expiration of contract, protected data can be returned to the School District or destroyed (per School District's preference). To return data to the District, Great Minds will create an SFTP for manual data transfer. When data destruction is requested by a customer or otherwise dictated by agreement terms, we perform an obfuscation of data. With this process we remove all references to PII or customer-specific information. We can provide output of the database scripts upon request.

- 4.) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected:

All requests to review personally identifiable information should be made by contacting the District who will confirm the relationship of the requestor and direct Great Minds to conduct the review.

- 5.) Where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data privacy and security risks mitigated:

Data is stored in US-based Amazon Web Services data centers (AWS). AWS data centers have been designed, constructed, and operated to restrict unauthorized users both at the perimeter and ingress of the facilities. Great Minds employs automated mechanisms to detect security incidents and leverages in-house SIEM for primary security monitoring and alerting. As a secondary or backup tool, we use our CSP in-house tools to detect anomalies, examine specific data points, and detect rare occurrences that seem suspicious.

- 6.) Address how the data will be protected using encryption while in motion and at rest.

Data is encrypted in transit (including via web interface) at TLS 1.2+ and at rest at AES-256.

7.) Third-party contractors are also required to:

- a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
- b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
- c. Not use educational records for any other purpose than those explicitly authorized in the contract;
- d. Not disclose personally identifiable information to any other party without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order;
- e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
- f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law 2-d:
- g. Notify the Northern Adirondack Central School District of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
- h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
- i. Provide a signed copy of this Bill of Rights to the Northern Adirondack Central School District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8.) This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

The Northern Adirondack Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Northern Adirondack School District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third party contractor. The district will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy.
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R).
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov.data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to (Data Protection Officer, Michael Loughman 518-594-3962 mloughman@nacs1.org Northern Adirondack Central School PO Box 164 Ellenburg Depot, NY 12935. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov.data-privacy-security>, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 5178-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting Michael Loughman 518-594-3962 mloughman@nacs1.org Northern Adirondack Central School PO Box 164 Ellenburg Depot, NY 12935 or can access the information on the district's website (www.nacs1.org).

BY THE VENDOR:

Donna M. Brown

Name (Print)

Signature

Interim General Counsel

Title

Date

NORTHERN ADIRONDACK CENTRAL SCHOOL DISTRICT DATA SECURITY AND PRIVACY POLICY:

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The Northern Adirondack Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy district.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the protections of "personally identifiable information" of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal "Personally/Identifiable Information" under Education Law §2-d

A. General Provisions

PII as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. *PII* as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of personally identifiable information (*PII*) by the district benefits students and the district (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, *PII* will not be included in public reports or other documents.

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500. Student Records.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the district's website at NACS1.org and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
 - a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
 - b. unless required by statute or court order and the third party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;
7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Privacy Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery .

The district will notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or

cause further disclosure of PII by disclosing an unfixed security vulnerability, the district will notify parents, eligible students, teachers and/or principals within seven calendar days after the security vulnerability has been remedied. or the risk of interference with the law enforcement investigation ends.

The Superintendent in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

II. "Private Information" under State Technology Law §208

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation. which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the district must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref:

1120, District Records

5500, Student Records

8630, Computer Resources and Data Management

Ref:
State Technology Law §§201-
208 Labor Law §203-d
Education Law
§2-d 8 NYCRR
Part 121

Adoption Date: April 20, 2020
Classification:
Revised Dates: ; **03.20**

Record of Signing

For Great Minds PBC
Name Donna M. Brown
Title Interim General Counsel

Donna M. Brown

Signed on 2024-09-11 15:20:34 GMT

Secured by Concord™
DocumentID: 02xewTPnvdSqZpUaAl9Bmp
SigningID: 02xewTPnpakaqVXydcZDDy
Signing date: 9/11/2024
IP Address: 136.226.107.1
Email: donna.brown@greatminds.org