West Irondequoit Central School District ("District")

Data Privacy Agreement for Vendors / Contractors / Service Providers

This Agreement supplements the underlying Contract to which it is attached to ensure that the underlying Contract for products or services to be provided to the District conforms to the requirements of New York State Education Law Section §2-d and related Regulations of the Commissioner of Education. To the extent that any term of the Contract conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

As used in this Agreement, **"Protected Data"** means all Personally Identifiable Information (PII) as defined in New York Education Law Section §2-d that Service Provider receives from District pursuant to the Contract. Examples of Protected Data include, but are not limited to, names, e-mail addresses, ID numbers, date of birth.

1. **Data Privacy**
   Service Provider agrees that the security, confidentiality, and integrity of Protected Data in its custody shall be maintained in accordance with state and federal laws that protect the confidentiality of Personally Identifiable Information, and also in accordance with District's Parents Bill of Rights for Data Security and Privacy, provided below.

2. **Data De-Identification**
   Service Provider may use de-identified data (i.e., Protected Data that has been de-identified so that it no longer qualifies as Protected Data) for product development, research, or similar purposes. De-identified data must have all direct and indirect personal identifiers removed. Furthermore, Service Provider agrees not to attempt to re-identify any de-identified data, and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification.

3. **Marketing and Advertising**
   Service Provider will not use any Protected Data to advertise or market to students, their parents, faculty or staff. The exclusive purpose for which Service Provider is being provided access to Protected Data is for providing the District with the functionality of the Products or Services accessed by the District pursuant to the Contract. Protected Data received by Service Provider, or by any assignee of Service Provider, from the District shall not be sold or used for marketing purposes.

4. **Data Sharing**
   Service Provider agrees that it will disclose Protected Data received from the District only to those officers, employees, and agents of Service Provider who need access to provide the contracted services. Service Provider further agrees to ensure that subcontractors or other entities to whom the Service Provider discloses Protected Data will abide by all applicable Protected Data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations.

5. **Data Privacy Training**
   Service Provider agrees that any of its officers or employees, and will require that any officers or employees of any assignee or subcontractor who have access to Protected Data, will receive training on the federal and state laws governing confidentiality of such Protected Data prior to receiving access to that Protected Data.

6. **Access and Correction**
   Service Provider agrees to support access to and correction of Protected Data by the District, including, when applicable, in response to a request by a District student or their authorized parent or guardian, consistent with the Family Educational Rights and Privacy Act (FERPA).

7. **Data Use and Collection**
   Service Provider will only collect and use Protected Data to provide the District with the Products

or Services contracted for by the District. Service Provider will disclose, in a manner easy for parents to understand, what types of student personal information is collected and for what purpose.

8. **Rights and Licenses to Data**
   Service Provider has a limited, non-exclusive license solely for the purpose of performing its obligations under the Contract and this Agreement. This Agreement does not give Service Provider any rights, implied or otherwise, to Protected Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Protected Data.

9. **Data Transfer or Destruction**
   Service Provider will ensure that all Protected Data in its possession and in the possession of any subcontractors, or agents to which the Service Provider may have transferred Protected Data, are destroyed or transferred to the District upon expiration of this Agreement without a successor contract in place, or upon request from the District.

10. **Data Protection**
    a. Service Provider will take reasonable measures aligned with industry standards, state and federal regulations such as Ed Law Section 2-d and related Commissioner's Regulations, and the NIST Cybersecurity Framework and reasonably designed to protect the privacy and security of Protected Data in Service Provider's possession, while it is stored and in transit. Such measures include, but are not necessarily limited to, encryption technology, firewalls, and password protection.
    b. Service Provider will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.
    c. Service Provider will conduct periodic risk assessments, remediating any identified security vulnerabilities in a timely manner.
    d. Service Provider will maintain a written incident response plan, to include prompt notification of the District in the event of a security or privacy incident, as well as best practices for responding to a breach of Protected Data.
    e. Service Provider agrees to share its incident response plan with District upon request.
    f. In the event of a breach or unauthorized release of Protected Data by the Service Provider or its subcontractor, the Service Provider will notify the District of the breach in the most expedient way possible and without unreasonable delay, but not more than 7 calendar days from awareness of incident. The Service Provider and the third party contractor may be subject to penalties as outlined in Education Law §2-d.
    g. Service Provider will ensure by contractual agreements or other legally binding measures that any subcontractor, assignee, or agent (including any Hosting Service Provider) to whom Service Provider discloses Protected Data will comply with the same data security and privacy standards required of Service Provider under this agreement and applicable state and federal laws.

References:

- https://studentprivacy.ed.gov/audience/education-technology-vendors
- http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf
- https://www.westirondequoit.org/UserFiles/Servers/Server_228510/File/DISTRICT/Parents_Bill_of_Rights.pdf
- https://www.nysenate.gov/legislation/laws/EDN/2-D
- http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/proposed-part-121-for-pii.pdf

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The West Irondequoit Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and 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.
4. A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/student-data-privacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure. Complaints may also be submitted to the District's Data Protection Officer by writing to: Data Protection Officer, West Irondequoit Central School District, 45 Cooper Road, Rochester, NY 14617.

APPENDIX

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 West Irondequoit 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 or 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 this 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;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, 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; Education Law Section 2-d);
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);
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;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the NYSED Chief Privacy Officer. Changes/Additions are also anticipated as NYSED releases further guidance documents.

Supplemental information describing third-party vendors engaged in data sharing and confidentiality agreements with West Irondequoit Central School District can be found at: https://dpit.riconedpss.org/billofrights/02d9d2af98c045c501f3.

West Irondequoit Central School District

Data Privacy Supplemental Information

Service Provider: Apex Learning Inc. Date: 6/4/2020

What protected data is stored? Service Provider may store Student Data in connection with its performance of the services contracted for by the District.

For what purpose(s) will this data be used? Protected Data received by Service Provider under its Contract with the District will be used to provide the District with the services described in the Contract.

What will happen to the data at the expiration of the contract/agreement? Once the Contract between Service Provider and District has ended, Service Provider will delete, destroy or de-identify (such that it no longer qualifies as Personally Identifiable Information) all Protected Data remaining in possession of Service Provider.

How may the accuracy of data be challenged? Eligible students, or student parents or guardians, may challenge the accuracy of any Protected Data in Service Provider's possession by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of their PII (as defined under NY Section 2-d) by following the District's appeal process.

Where is the data stored and how is it protected? Protected Data received by Service Provider under its Contract with the District will be stored on systems maintained by Service Provider, or by a data center vendor under contract with Service Provider, in a data center facility located within the United States.

How is the data protected using encryption while in motion and at rest? Service Provider will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Provider Statement: We agree to abide by the terms above.

Name: Chuck Lanphier **Title:** VP, Client Services

Signature:  **Date:** 6/4/2020

Revised 2/20/2020