

STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE, NEW YORK, RHODE ISLAND AND VERMONT

MA-ME-NH-NY-RI-VT-NDPA, Standard Version 1.0

Worcester Public Schools

and

Eduready360 LLC

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between: Worcester Public Schools, located at 20 Irving Street, Worcester, MA 01609 (the “Local Education Agency” or “LEA”) and Eduready360 LLC, located at 128 Innovative Lane, Suite 202, Latrobe, PA 15650 (the “Provider”).

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “Services”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: John Lohr, Eduready360 Title: Chief Customer Success Officer

Address: 128 Innovative Lane, STE 202, Latrobe, PA 15650

Phone: 7247771571

Email: john@eduready360.com

The designated representative for the LEA for this DPA is:

Marco Andrade, Ph.D., Director, Office of Research and Accountability
Worcester Public Schools
20 Irving Street, Rm. 202 | Worcester, MA 01609
508-799-3060
andradem@worcesterschools.net

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Worcester Public Schools

By: *Marco Andrade*
Marco Andrade (Jan 24, 2024 15:53 EST)

Date: 1/24/24

Printed Name: Marco Andrade

Title/Position: Director of Research and Accountability

Eduready360 LLC

By: *John C Lohr*

Date: 1/24/2024

Printed Name: John C Lohr

Title/Position: Chief Customer Success Officer

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2)

research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security

programs and measures that augment or are in addition to the Cybersecurity Framework in Exhibit "F". Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
 - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
 - (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as Exhibit "E"), be bound by the terms of Exhibit "E" to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

CTE-360, a cloud-based software solution to track all aspects of student work-based learning experiences.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X

Category of Data	Elements	Check if Used by Your System
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	X
	Student course grades/ performance scores	X
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal

records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"

Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.

Date of birth.

Personal street address.

Personal email address.

Personal telephone number

Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
- (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries)	X
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	X
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	X
	Teacher calendar	X
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	X
	Other teacher work data -Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."
7. To amend Article II, Section 6 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA's Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and its subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department’s Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Contractor to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider’s expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider’s privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the

incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident.

Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

- i. The name and contact information of the reporting LEA subject to this section.
- ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
- v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
- vi. The number of records affected, if known; and
- vii. A description of the investigation undertaken so far; and
- viii. The name of a point of contact for Provider.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

(6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.

Exhibit “J”
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at:

See attached Data Privacy & Information Assurances document.

Information Assurance

Information Assurance (IA) is the practice of managing information-related risks and the steps involved to protect information. These are the measures we use to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of data and systems by incorporating protection, detection, and reaction capabilities.

Integrity

Integrity means all information systems are protected and not tampered with. At Eduready360, we aim to maintain integrity by taking measures to prevent any form of unauthorized access, both internally and externally, to information systems and data. This includes requiring all of our staff to attend annual training to improve awareness on topics such as phishing and ransomware to reduce the likelihood of systems being breached and data being exposed. Additionally, accounts that have been inactive for more than one year are automatically disabled to limit potential attack vectors.

Availability

Availability means those who need to access information are provided with dependable access to it. We ensure availability by utilizing redundant, scalable, highly available services to store data and host our applications. We make use of tools such as AWS CloudWatch to monitor the health of our infrastructure. Additionally, we use services like [Sentry](#) to notify us of fatal errors in the application's code so we can proactively address issues before they are even reported to us. All code changes are tested in a sandbox and immutable deployment methods are used to ensure there is no downtime when changes are deployed to a production environment.

Authentication

Authentication involves ensuring those who have access to information are who they say they are. Internally, we require the use of multi-factor authentication wherever possible and require the use of strong passwords for administrative access to information. We also provide Single Sign On (SSO) options via third-party identity providers to allow our clients to have more control over the authentication process. Passwords are never stored in plaintext. They are hashed and salted using one-way encryption for the highest level of security. Sessions also automatically expire after a specified period of inactivity to decrease the likelihood of unauthorized access. All login attempts are logged, including the IP address of origin, and accounts are locked if there are too many failed attempts to prevent intrusions.

Confidentiality

Confidentiality means that only those with authorization may view protected information. This is closely mirrored by the six data processing principles of the General Data Protection Regulation (GDPR), whereby personal data must be processed in a secure manner using appropriate technical and organizational measures. We have a number of controls and security roles within our applications to limit access to confidential and protected information.

Nonrepudiation

Nonrepudiation means someone with access to your organization's application cannot deny having completed an action within the system. This is accomplished by storing information in our database that can be used to create a reliable audit trail of all user actions. We do include the ability to "Log in As" another user, but all actions taken are attributed to the original user.

Data Privacy & Security

Data privacy consists of the policies and processes that dictate how we collect, use, share and store your personal data. This is governed by state/province and/or federal laws that apply to specific industries and/or locations. More detailed information about how we comply with these mandates can be found in our Privacy Policy, which can be accessed from this link: <https://eduready360.com/privacy-policy/>.

Personally Identifiable Information

The U.S. Family Educational Rights and Privacy Act (FERPA) regulates access to student education records, imposing strict requirements on how electronic records and personally identifiable information are stored and protected. The term "student" refers to any person attending or seeking to enroll in an educational agency, and according to the definition provided by FERPA, the term "personally identifiable information" ("PII") includes, but is not limited to:

- (a) The student's name;
- (b) The name of the student's parent or other family members;
- (c) The address of the student or student's family;
- (d) A personal identifier, such as the student's social security number, student number, or biometric record;
- (e) Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name;
- (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

The confidentiality and privacy provisions of FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that use random identifiers), aggregated data (e.g., data reported at the school district level), or anonymized data that could not be used to identify a particular student is not considered to be PII.

Protected Data

Protected Data is defined as personally identifiable information of students from student education records, as defined by FERPA, as well as teacher and administrator data. Eduready360 agrees that the confidentiality of Protected Data shall be maintained in accordance with state and federal laws and the educational agency's policies on data security and privacy that protect the confidentiality of personally identifiable information.

Purpose of Data Collection

The exclusive purpose for which Eduready360 is being provided access to protected data is to enable our clients to make use of the services we provide that relate to an educational purpose. Any data obtained from our clients will not be sold or used for marketing purposes. Every use and disclosure of personally identifiable information shall be for the benefit of students and the educational agency.

Limiting Access to Protected Data

We take steps to minimize our collection, processing, and transmission of protected data. Access to protected data is automatically limited to users of our applications based upon their user type (student, guardian, teacher, staff, or school admin) and the specific security roles assigned to those users (ie. Work-Based Learning Coordinator). For instance, teachers are only permitted to view students that are enrolled in classes that they teach and employers are not given user credentials to log in to applications that store student data.

Additionally, we do not provide a way to store unnecessary PII and directory information in our applications, such as Social Security Numbers.

As defined in our [Privacy Policy](#), we will never sell or release a student's personally identifiable information for any commercial purpose. Safeguards aligned with industry standards and best practices are also in place to protect student PII when it is stored and transferred.

Complaints & Challenges to Data Accuracy

Users have the right to request amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA. If a parent, student, teacher, or administrator wishes to challenge the accuracy of the protected data that we have collected, they can do so by submitting their request via email, live chat, or phone. This can be done using this link: <https://eduready360.com/contact-us/>. They can also contact the school or school district directly. Each challenge we receive will be processed through the procedures provided by the client or by the student's district of enrollment in accordance with state and federal laws. We may rely on schools and school districts to make the requested changes since they are in the best position to make corrections to students'

education records, especially if the data in question was obtained via an integration with a school-owned student information system.

Parents and students also have the right to have complaints about possible breaches and unauthorized disclosures of PII addressed and to be notified in accordance with applicable laws and regulations. Complaints may be submitted in accordance with section 11 of our [Privacy Policy](#).

Protected Data Handling after Termination of Services

All data entered or obtained from our clients is owned by them. When a contract with a school expires, this data will be retained for up to 1 year after the termination of services. Upon request, this data will be delivered to the client in the form of an export of all database content and files that we have stored on their behalf.

Upon expiration of an agreement, Eduready360 will assist the client in exporting all protected data previously received from client, and Eduready360, at the client's request, will thereafter securely delete any copy of the data remaining in Eduready360's possession or control. If data is to be maintained by Eduready360 for federal and/or state reporting purposes, such data will remain in an encrypted format and stored in a secure facility located within the United States of America.

Breach of Confidentiality or Security

Upon receipt of a complaint or other indication that Eduready360 may have improperly disclosed (lost, accessed, or obtained) protected data in violation of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) or other federal or state law applicable to such information accessed or obtained by an unauthorized individual, the following process shall be followed:

1. Eduready360 will immediately notify the educational agency of the breach in the most expedient way possible and without unreasonable delay.
 - a. This notification shall occur within 48 hours of becoming aware of the potential breach and include the date, estimated date, or date range of the loss or disclosure; the protected data that was or is reasonably believed to have been lost or disclosed; and remedial measures taken or planned in response to the loss or disclosure.
2. Eduready360 will immediately take all legally required, reasonable, and customary measures to remediate and prevent further access to and disclosure of protected data. Eduready360 will provide free help desk support to address questions by affected parties and/or provide monitoring services if necessary given the nature and scope of the loss or disclosure.
3. The school will be permitted to designate an authorized representative to fully participate in the investigation of the incident. This includes examining and inspecting data center facilities and Eduready360's records. Eduready360 will also facilitate obtaining documentation or testimony from any party relating to the alleged improper disclosure of protected data.
4. Eduready360 will NOT directly contact impacted parents, legal guardians, or students unless expressly requested by the educational agency. The educational agency will be responsible for notifying any

impacted individuals and Eduready360 will cooperate with all efforts to communicate to the affected parties.

5. Eduready360 shall indemnify and hold harmless the educational agency from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by Eduready360 or any of its officers, directors, employees, agents or representatives of the obligations of Eduready360's or its Authorized Representatives under this provision or under a Confidentiality Agreement, as the case may be.

Where is my data stored and how is it protected?

Your data will either be stored in file objects (buckets) or in a database. We provide strong administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of all electronic records.

All data collected is protected in accordance with industry standards and best practices, including the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF). Protections include, but are not limited to, encryption, firewalls, complex passwords, multi-factor authentication, and database isolation.

We also safeguard all confidential information from disclosure to non-essential personnel within and outside of our organization to comply with the privacy laws that protect such information, including student education records protected under The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).

File uploads, backups, and database records are stored using fully secure and redundant third-party data centers located across multiple Availability Zones (AZ) in the US East 1 (Ashburn, Virginia) region.

Data Ownership and Disclosure

Our [Terms of Service](#) grant schools exclusive ownership and control of their electronic records as required by FERPA. All data stored remains the exclusive and confidential property of the educational institution.

File Storage (AWS S3 Buckets)

The data centers we use for storing file objects guarantee 99.999999999% data durability and are also certified for SOC 2, ISO 27001, and PCI-DSS compliance. Copies of compliance reports can be provided if needed. This third-party service is built and managed according to security best practices and standards, with U.S. Department of Education PTAC data security guidelines in mind. This includes the physical security of its data centers; strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encryption of data at rest and in transit to safeguard protected data.

Physical Security

Files are hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility, both indoors and

outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Advanced network security elements, including firewalls and other boundary protection devices monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to infrastructure and services.

Data Privacy and Security

To prevent unauthorized disclosure of protected data, strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant permissions to users or groups of users. Data is also encrypted at rest using AES-256 encryption and in transit using SSL/TLS to prevent record leakage. All communications with data centers are transmitted using HTTPS to protect data in transit.

Data Durability and Protection

The cloud storage we utilize is engineered for extreme data durability and integrity. They provide eleven 9s (99.999999999%) object durability, protecting data against hardware failures and media errors. In addition, we also utilize a data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone, including data center staff. Data immutability protects the integrity of electronic student education records, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Database Storage (AWS RDS)

We rely on the [Aurora PostgreSQL engine of the Relational Database Service \(RDS\)](#) provided by Amazon Web Services (AWS) for database storage. RDS allows us to scale your database's compute and storage resources with little or no downtime to ensure high availability. We also use automated backups, database snapshots, and automatic host replacement, and multi-AZ synchronous data replication across Availability Zones with automatic failover, to enhance the reliability and integrity of this service.

Network & Database Isolation

Our RDS database instances also run in a Virtual Private Cloud (VPC), which isolates the database instances from unauthorized devices/networks. RDS access is only permitted to other AWS resources that are on the same Virtual Network. Security groups are used to control what IP addresses or Amazon EC2 instances can connect to our databases. Firewalls also prevent any database access except through rules specified by an associated security group that allow only authorized, internal access. Public access to databases is not possible. Additionally, we create separate, isolated databases for each of our clients to prevent unauthorized or accidental access to information. Database passwords are also randomized and unique to each client.

Encryption at Rest and in Transit

The database engine in use also provides encryption of data at rest and encryption in transit. Data that is encrypted at rest includes the underlying storage for DB instances, its automated backups, logs, read replicas, and snapshots. The industry standard AES-256 encryption algorithm is used to encrypt your data on the server that hosts your Amazon RDS DB instances. After your data is encrypted, Amazon RDS handles authentication of access and decryption of your data transparently with a minimal impact on performance. Data that is in transit between the source and the read replicas is also encrypted using SSL/TLS, even when replicating across AWS Regions.

Data Security Compliance

Independent auditors regularly test and verify the effectiveness of security as part of the AWS compliance programs in place.

Restricted User Access

We use AWS Identity and Access Management (IAM) policies to assign permissions that limit who is allowed to manage Amazon RDS resources. Only one account has access to create, describe, modify, and delete DB instances, tag resources, or modify security groups and this account is protected by multi-factor authentication and a complex, secure password. We create an individual IAM user for each person who manages Amazon RDS resources and do not use AWS root credentials to manage Amazon RDS resources. Each user is granted the minimum set of permissions required to perform his or her duties. IAM credentials and keys are also rotated regularly.

Availability and durability

We make use of the Amazon Aurora database engine that automatically grows the size of your database volume as your database storage needs grow. Storage scaling is on-the-fly with zero downtime. We also utilize Read Replicas that are able to elastically scale beyond the capacity constraints of a single DB instance for read-heavy database workloads.

Automated Backups

We use the automated backup feature of Amazon RDS to enable point-in-time recovery for all database instances. Amazon RDS backs up your database and transaction logs and store both for 21 days. This allows us to restore your database instance to any time during your retention period, up to the last five minutes.

Patch Management

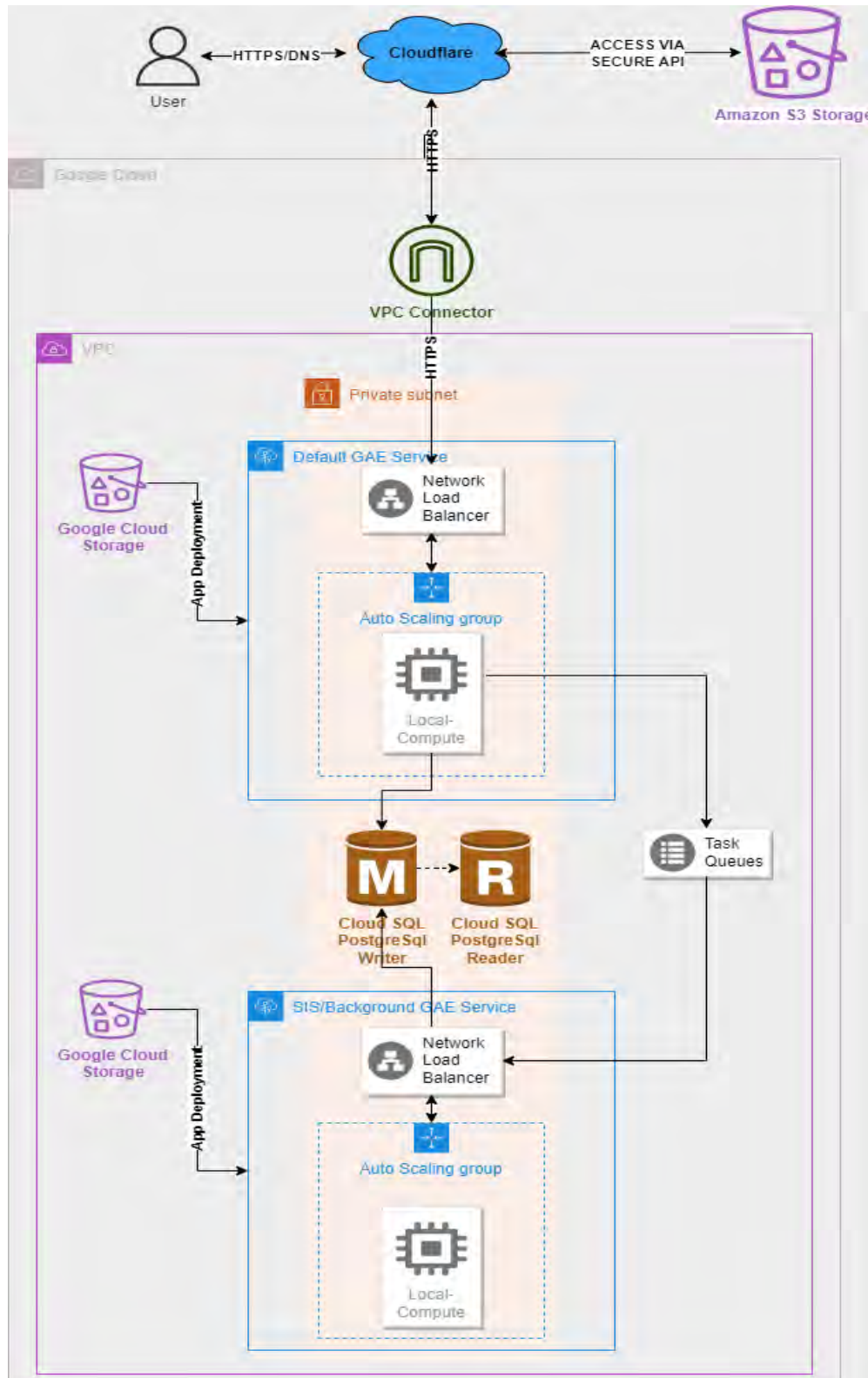
We update the database engine (Aurora PostgreSQL) to the most current minor version automatically during scheduled maintenance windows to ensure the latest security and functionality fixes are being applied. We utilize the Auto minor version upgrade feature provided by AWS to accomplish this. Unlike major version upgrades, minor version upgrades include only changes that are backward-compatible with previous minor versions (of the same major version) of the DB engine. Major version updates are only performed after application testing in a development environment has been completed to ensure there is no disruption to service.



128 Innovation Lane, STE 202
Latrobe, PA 15650
(412) 348-6360

The PostgreSQL community releases a new major version yearly, with a defined end of life (EOL) policy of older major versions. This allows us to make version and upgrade decisions well into the future. The community EOL policy is to support a major version for 5 years after its initial release. After the fifth year, a major version has one final minor release containing any fixes, and is then considered EOL and no longer supported. It is our goal to upgrade major versions at least 1 year prior to the scheduled EOL date.

Our Infrastructure



Web Application Infrastructure

We rely on the App Engine, fully managed, cloud environment provided by Google Cloud Platform (GCP) for hosting, deploying, and scaling all of our web applications and services (including CTE-360, Jobready WBL, and K12-360). App Engine automatically handles the deployment, capacity provisioning, load balancing, auto-scaling, and application health monitoring. This ensures high availability and continuous access to your data.

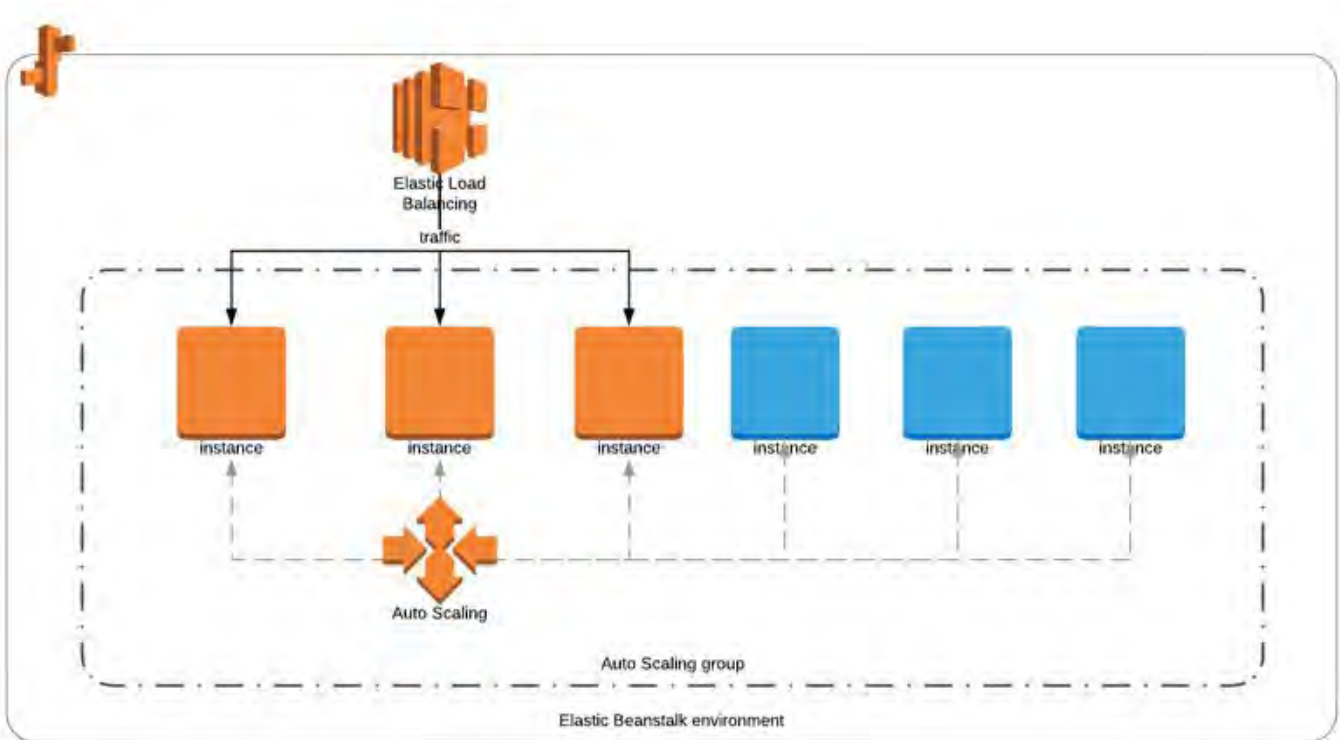
App Engine provides managed platforms that support running web applications developed for specific programming languages, frameworks, and web containers. App Engine provisions and operates the infrastructure and manages the application stack for us. To ensure the underlying platform is up-to-date with the latest patches and updates, we dedicate time and personnel to updating the platform version to the most current release (if one exists) once every two weeks during scheduled maintenance time. The platform branch itself is updated less frequently since application code may need to be updated and tested to ensure compatibility with these changes. For instance, upgrading major PHP versions could break core functions of the web application. The web application will be tested in a development environment and upgrades to the platform branch will be made prior to the End of Support date [listed here](#), once testing indicates the application is compatible with the new platform branch.

Our App Engine instances run using Google's second-generation standard runtime environments, which provide a security-focused, stable, and high-performance execution environment to develop and run cloud applications.

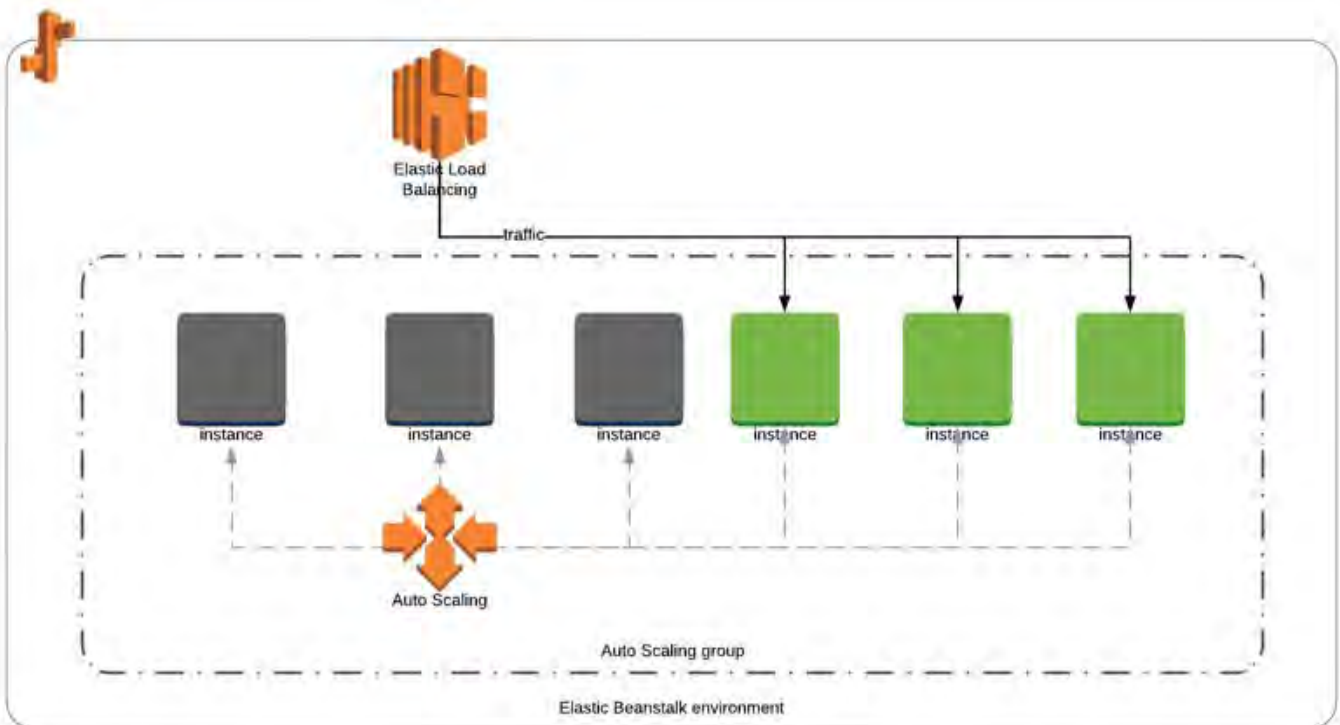
Deploying Updates to Eduready360 Applications

Another factor that can affect availability is the stability of the application itself. To ensure the application is as stable as possible, all code changes are tested in a development environment before they are deployed to a production environment. However, no matter what precautions are taken, there is always the possibility of unforeseen consequences. Our philosophy when it comes to updates is to be as adaptable as we can be. Oftentimes, this means we will make frequent updates. If a bug is discovered, we want to be flexible enough to quickly resolve the issue and deploy a fix with as little down time as is possible. We also want to be able to deploy new features and improvements as soon as possible to make the user experience the best it can be.

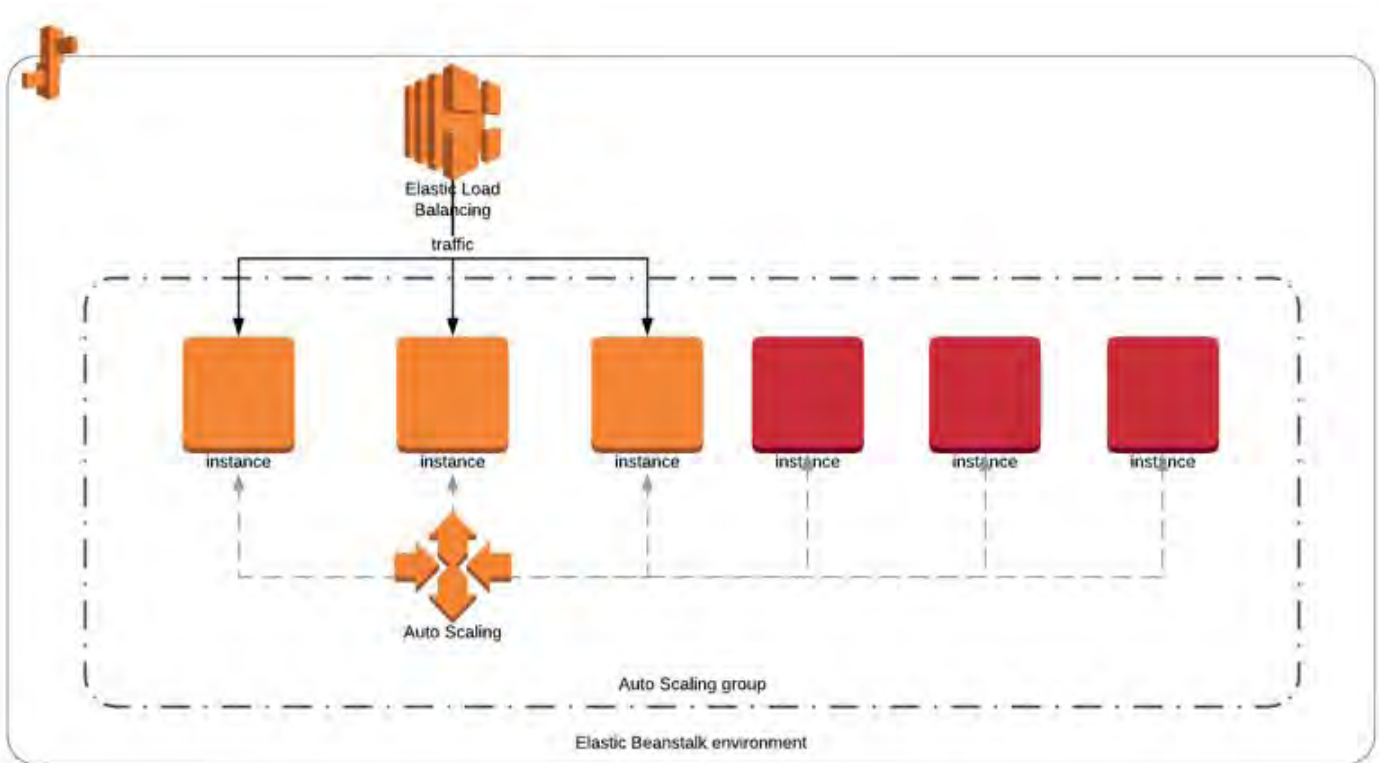
We deploy changes to Google Cloud using an immutable deployment method. This launches new instances and duplicates the size of the autoscaling group for a short period, deploying the latest version of code in new instances and terminating the old group after success. In the case of a deployment failure, the new instances will be terminated without affecting availability. This ensures there is never any downtime during deployments and allows us to make frequent changes without the loss of availability.



1. Deployment starts by duplicating the instances and deploying the app in new instances



2. After deployment succeeds, older instances are terminated.



In case of failure, the new instances is terminated and traffic is not effected.

Integrations With Other Systems

At your discretion, our applications may be configured to gather data from third-party information systems, such as a Student Information System (SIS) or Learning Management System (LMS). These integrations are meant to alleviate the burden of creating and maintaining user accounts and to keep student enrollment records current in our applications.

To limit the amount of data that we store in our database, and to therefore limit the potential impact of a data breach, our application can be configured to only store student information for students that are enrolled in courses you have chosen to sync. The courses that we sync are defined on the Global Settings page. We also do not store sensitive information that we do not need (such as Social Security numbers, birth dates, ages, etc.).

Typically, these integrations are done using an Application Programming Interface (API) such as OneRoster. However, we also support automated SFTP uploads. To limit the potential exposure of this information, data is secured in transit via SSL or TLS, very complex passwords are used, and if necessary, authentication credentials are split up when communicated to our clients via multiple methods of communication (email, phone, text messages, etc.).

What SIS Data is Transferred?

We only request rostering data from the SIS. This does not include demographic information, grades, or attendance information. We adhere to the OneRoster specifications for data obtained whether this sourced from a CSV upload or from an API call. What follows is the data that we require for a SIS integration.

academicSessions.csv

This file represents the AcademicSessions dataset from the OneRoster specification.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	SourcedId of this academicSession.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
title	Yes	String	Name or title of the academic session.
type	Yes	Enumeration	See section 4.13.7 [OneRoster, 20a] for the enumeration list.
startDate	Yes	Date	Inclusive start date for the academic session.
endDate	Yes	Date	Exclusive end date for the academic session.
parentSourcedId	No	GUID Reference.	SourcedId of the parent of this academic session.

schoolYear	Yes	Year	The school year for which the academic session contributes. This year should be that in which the school year ends. (Format is: YYYY).
------------	-----	------	---

classes.csv

This file represents the Class dataset from OneRoster specification.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	Unique ID for the class. SourcedId is used in other files and must be unique across all classes.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
title	Yes	String	Name of this class.
grades	No	List of Strings	Grade(s) for which the class is attended. The permitted vocabulary is from CEDS (Version 5) and the 'Entry Grade Level' element https://ceds.ed.gov/CEDSElementDetails.aspx?TermId=7100
courseSourcedId	Yes	GUID Reference.	SourcedId of the course of which this class is an instance.
classCode	No	String	Human readable code used to help identify this class.
classType	Yes	Enumeration	See section 4.13.1 [OneRoster, 20a] for the enumeration list.
location	No	String	Human readable description of where the class is physically located.

schoolSourcedId	Yes	GUID Reference.	SourcedId of the Org that teaches this class of OrgType "school".
termSourcedIds	Yes	List of GUID References.	SourcedId of the terms (the academicSessions) in which the class is taught.
subjects	No	List of Strings	<p>Subject name(s) in human readable form. If the 'subjectCodes' attribute is present then the subjects and subjectCodes lists must have the same length and have order significance</p> <p>The vocabulary is from SCED (School Codes for the Exchange of Data) (Version 4) for the "Course Title" field: http://nces.ed.gov/forum/SCED.asp</p> <p>If the value of the "Course Title" contains commas, then those commas must be removed.</p> <p>For example, the "Course Title" for "SCED Course Code" "03210" is "Science, Technology and Society". This must be represented as "Science Technology and Society".</p>
subjectCodes	No	List of Strings	<p>Subject codes(s) in machine readable form. If more than one subject code is needed, use double quotes, and separate with commas (per RFC 4180). If the 'subjects' attribute is present the two lists must have the same length and have order significance.</p> <p>For deployments in the USA this vocabulary SHOULD be a School Courses for the Exchange of Data (SCED) code: http://nces.ed.gov/forum/SCED.asp</p>
periods	No	List of Strings	<p>The time slots in the day that the class will be given. If more than one period is needed, use double quotes, and separate with commas (per RFC 4180).</p> <p>Examples: 1; "1,3,5"</p>

courses.csv

This file represents the Course dataset from OneRoster.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	Unique ID for the course.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
schoolYearSourcedId	No	GUID Reference.	SourcedId of an AcademicSession with type of "schoolYear".
title	Yes	String	Name of the course.
courseCode	No	String	Human readable course code.
grades	No	List of Strings	Grade(s) for which the class is attended. The permitted vocabulary is from CEDS (Version 5) for the 'Entry Grade Level' element https://ceds.ed.gov/CEDSElementDetails.aspx?TermId=7100
orgSourcedId	Yes	GUID Reference.	SourcedId of an org to which this course belongs.

subjects	No	List of Strings	<p>Subject name(s) in human readable form. If the 'subjectCodes' attribute is present then the subjects and subjectCodes lists must have the same length and have order significance</p> <p>The vocabulary is from SCED (School Codes for the Exchange of Data) (Version 4) for the "Course Title" field: http://nces.ed.gov/forum/SCED.asp</p> <p>If the value of the "Course Title" contains commas, then those commas must be removed.</p> <p>For example the "Course Title" for "SCED Course Code" "03210" is "Science, Technology and Society". This must be represented as "Science Technology and Society".</p>
subjectCodes	No	String	<p>Subject codes(s) in machine readable form. If the 'subjects' attribute is present then the subjects and subjectCodes lists must have the same length and have order significance.</p> <p>For deployments in the USA this vocabulary SHOULD be a School Courses for the Exchange of Data (SCED) code: http://nces.ed.gov/forum/SCED.asp.</p>

orgs.csv

This represents the Org dataset from OneRoster.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	Unique id for the organization. SourcedId is used in other files and must be unique across all organizations.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
name	Yes	String	Name of the organization.
type	Yes	Enumeration	See section 4.13.7 [OneRoster, 20a] for the enumeration list.
identifier	No	String	NCES ID National Center for Education Statistics) for the school/district.
parentSourcedId	No	GUID Reference.	SourcedId of an Org representing the Parent organization.

enrollments.csv

This represents the Enrollment dataset from OneRoster.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	Unique identifier of this enrollment.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
classSourcedId	Yes	GUID Reference.	SourcedId of the Class.
schoolSourcedId	Yes	GUID Reference.	SourcedId of an Org with type 'school'.
userSourcedId	Yes	GUID Reference.	SourcedId of the User.
role	Yes	Enumeration	See section 4.13.5 [OneRoster, 20a] for the enumeration list. The ONLY permitted values are: { administrator proctor student teacher }.
primary	No	Enumeration	Permitted values: { "true" "false" }. Applicable only to teachers. Only one teacher should be designated as the primary teacher for a class in the period defined by the begin/end dates.
beginDate	No	Date	The start date for the enrollment. This date must align with the associated academic session (term) identified in the class.

endDate	No	Date	The end date for the enrollment (exclusive). This date must align with the associated academic session (term) identified for the class.
---------	----	------	---

users.csv

This represents the Users dataset from OneRoster.

Column Field Header	Required	Format	Description
sourcedId	Yes	GUID	Unique ID for the user. SourcedId is used in other files and must be unique across all users.
status	Yes for Delta	Enumeration	See section 4.13.8 [OneRoster, 20a] for the enumeration list. This <i>MUST NOT</i> be used for the Bulk mode.
dateLastModified	Yes for Delta	DateTime	The date that this record was last modified. This <i>MUST NOT</i> be used for the Bulk mode.
enabledUser	Yes	Enumeration	Permitted values: { "true" "false" }. 'false' denotes that the user is an active record but system access is curtailed according to the local administration rules.
orgSourcedIds	Yes	List of GUID References.	SourcedIds of the Orgs to which this user belongs. (Note in most cases, it is expected that users will belong to a single school).
role	Yes	Enumeration	See section 4.13.5 [OneRoster, 20a] for the full enumeration list.

username	Yes	String	User name.
userIds	No	List of Strings	External machine-readable ID (e.g. LDAP id, LTI id) for this user. The ID must be accompanied by a type to indicate the nature of the Identifier. The Type and ID values are enclosed in '{}' with a colon used to separate the values. If more than one userId is needed, use double quotes, and separate with commas (per RFC 4180). Examples: {LDAP:Id} "{LDAP:Id},{LTI:Id},{Fed:Id}"
givenName	Yes	String	User's first name.
familyName	Yes	String	User's surname.
middleName	No	String	User's middle name (s). If more than one then they are separated by a space.
identifier	No	String	Identifier for the user with a human readable meaning.
email	No	String	Email address for the User.
sms	No	String	SMS address for the User.
phone	No	String	Phone number for the User.
agentSourcedIds	No	List of GUID References	SourcedIds of the Users to which this user has a relationship. If multiple IDs are required then use double quotes and separate with commas. Note: In most cases this will be for indicating parental relationships.

grades	Only for student records	String	Grade(s) for which a user with role 'student' is enrolled. The permitted vocabulary is from CEDS (Version 5) for the 'Entry Grade Level' element https://ceds.ed.gov/CEDSElementDetails.aspx?TermId=7100 .
password	No	String	The password for the user. This may or may not be an encrypted string. If encrypted, the system's processing must be aware of the encryption method.







Eduready360_Worcester_6State_VendorSigned

Final Audit Report

2024-01-24

Created:	2024-01-24
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA3D32pNHfrirjRU8XmW5_z2d8oKcw-TuX

"Eduready360_Worcester_6State_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-01-24 - 8:21:57 PM GMT- IP address: 108.35.203.7
-  Document emailed to andradem@worcesterschools.net for signature
2024-01-24 - 8:23:09 PM GMT
-  Email viewed by andradem@worcesterschools.net
2024-01-24 - 8:52:21 PM GMT- IP address: 131.239.115.250
-  Signer andradem@worcesterschools.net entered name at signing as Marco Andrade
2024-01-24 - 8:53:08 PM GMT- IP address: 131.239.115.250
-  Document e-signed by Marco Andrade (andradem@worcesterschools.net)
Signature Date: 2024-01-24 - 8:53:10 PM GMT - Time Source: server- IP address: 131.239.115.250
-  Agreement completed.
2024-01-24 - 8:53:10 PM GMT