

**NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT
VERSION (2019)**

Henniker School District – SAU 24

and

Tyler Technologies, Inc.

February 2, 2021

This New Hampshire Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Henniker School District, (hereinafter referred to as “LEA”) and Tyler Technologies, Inc. (hereinafter referred to as “Provider”) on February 2, 2021. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) pursuant to a License and Services Agreement dated February 10, 2020 (the “Underlying Agreement”) as described in Article I and Exhibit “A”; and

WHEREAS, in order to provide the Services described in Article I and Exhibit “A”, the Provider may collect, process, store or transmit, and the LEA may provide to the Provider, documents or data that are covered, as applicable, by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 34 CFR Part 99, Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, Provider’s Services may also be subject to several New Hampshire student and teacher data privacy laws, including, as applicable, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to amend the Underlying Agreement by entering into this DPA to ensure that the Services provided conform to the requirements of the privacy laws applicable to the Services and referred to above, and to establish implementing procedures and duties.

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

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 and Teacher Data (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to the Underlying Agreement described in Exhibit “A”, including compliance with all applicable federal and New Hampshire state privacy statutes, including, as applicable, the FERPA, PPRA, COPPA, IDEA, , RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these Services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) and Teacher Data (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA.
- 2. Nature of Services Provided.** The Provider has agreed to provide the digital educational services described in the Underlying Agreement.

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of Student Data and Teacher Data described in the Schedule of Data, attached hereto as Exhibit “B”.
4. **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 all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data, Teacher Data or any other Pupil Records transmitted to the Provider pursuant to the Underlying Agreement is and will continue to be the property of and under the control of the LEA, or of the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data, Teacher Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data, Teacher Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data, Teacher Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and applicable state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data and Teacher Data notwithstanding the above. The Provider will cooperate and provide access to Student Data and Teacher Data which Provider stores within ten (10) business days at the LEA’s request. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of the Services. Provider shall cooperate and respond within ten (10) business days to the LEA’s request for personally identifiable information in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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.** Provider shall, at the request of the LEA, transfer Pupil Generated Content, if any, stored by Provider, to a separate student account in an industry standard format.
4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data or Teacher Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA and shall cooperate with the LEA to collect the required information if Provider holds or maintains

any such Student Data or Teacher Data. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. Except as necessary to provide the Services, the Provider will not use, disclose, compile, or transfer the Student Data, Teacher Data, and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, or transfer the Student Data, Teacher Data, and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. The Provider will not sell the Student Data, Teacher Data, and/or any portion thereof and shall require that any Third Party that collects, processes or stores the Student Data or the Teacher Data in support of the Services shall agree to not sell the Student Data or Teacher Data. Student Data and Teacher 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.

5. **No Unauthorized Use.** Provider shall not use Student Data, Teacher Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data and Teacher Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws.** LEA shall provide Student Data and Teacher Data for the purposes of the DPA in compliance with the FERPA, PPR, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected 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 New Hampshire and Federal laws and regulations pertaining to the data privacy and security of the Student Data and the Teacher Data, including, as applicable, FERPA, COPPA, PPR, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.

2. **Authorized Use.** Student Data and Teacher Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as authorized under the statutes referred to in subsection (1), above.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data or Teacher Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data or Teacher Data pursuant to the DPA.
4. **No Disclosure.** De-identified information, as defined in Exhibit “C”, may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and Teacher Data and not to transfer de-identified Student Data and Teacher 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. Provider shall not copy, reproduce or transmit any Student Data or Teacher Data obtained under the Underlying Agreement and/or any portion thereof, except as necessary to fulfill the Underlying Agreement. 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.
5. **Disposition of Data.** To the extent feasible, Provider shall dispose or delete all personally identifiable Student Data and Teacher Data stored by Provider pursuant to the Underlying Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data in a standard data format to LEA or LEA’s designee on the date of termination of the Underlying Agreement according to a schedule and procedure as the Parties may reasonably agree. Upon a written request of the LEA, except for backups, the Provider will dispose or delete Student Data and Teacher Data within sixty days. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition, except for backups as outlined below. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Student Data and Teacher Data has been disposed. The duty to dispose of Student Data and Teacher Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. All backups will be deleted within one year. Backups will receive the same protections as all other Student Data under this DPA and the LEA may request in writing at any time the status of backups. The LEA may request within one year of termination of this DPA, the status of a backup and may request deletion of any restored LEA data.

The LEA may employ a “Directive for Disposition of Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will provide the LEA with any specified portion of the Student Data or Teacher Data in a standard file format within ten (10) business days of receipt of said request.

6. **Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data or Teacher Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to the 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 Services to the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards, to protect Student Data and Teacher Data collected, processed, transmitted or stored by Provider from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider with respect to any Student Data or Teacher Data which Provider collects, processes, stores or transmits pursuant to the Underlying Agreement are set forth below. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall secure its employees' usernames, passwords, and any other means of Provider gaining access to the Services or to Student Data and Teacher Data. Provider shall only provide access to Student Data and Teacher Data to employees or contractors that are performing the Services. Employees with access to Student Data and Teacher Data shall have signed confidentiality agreements regarding said Student Data and Teacher Data. For at least the past fifteen (15) years, all of Provider's employees have undergone criminal background checks prior to hire.
 - b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data or Teacher Data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall process, collect, transmit or store Student Data and Teacher Data pursuant to the Underlying Agreement and in a secure computer environment and not copy, reproduce, or transmit Student Data and Teacher Data obtained pursuant to the Underlying Agreement, except as necessary to fulfill the purpose of the Underlying Agreement. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.
 - c. **Employee Training.** The Provider shall provide recurring, periodic (no less than annual) industry standard security training to those of its employees who have access to Student Data or Teacher Data. LEA may email ITSO@tylertech.com if there are any security concerns or questions.
 - d. **Security Technology.** When Provider is hosting Student Data or Teacher Data, Provider will provide secure data transmission paths between each of LEA's workstations and Provider's servers. Any Student Data or Teacher Data hosted by Provider pursuant to the Underlying Agreement shall be hosted in an environment using a firewall that is periodically updated according to industry standards.
 - f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Senior Information Security Officer for the Student Data and Teacher Data received pursuant to the DPA.

- g. Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data and Teacher Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance assessments of Subprocessors to determine their compliance with this Article.
 - h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments of the Services and remediate any confirmed critical or high priority identified security vulnerabilities in a timely manner.
 - i. Intentionally Omitted.**
 - j. Audits.** Provider’s hosted Services are audited at least yearly in accordance with the AICPA’s Statement on Standards for Attestation Engagements (“SSAE”) No. 18. Provider has attained, and will maintain, SOC 1 and SOC 2 compliance, or its equivalent, for so long as LEA is timely paying for hosted Services. Upon execution of a mutually agreeable Non-Disclosure Agreement (“NDA”), Provider will provide LEA with a summary of Provider’s compliance report(s) or its equivalent. Every year thereafter, for so long as the NDA is in effect and in which LEA makes a written request, Provider will provide that same information. The Provider will cooperate reasonably with LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation performed by such state or federal agency of the Provider and/or delivery of Services to students and/or LEA and shall provide reasonable access to the records pertaining to the delivery of Services to the LEA by the Provider.
 - k. New Hampshire Specific Data Security Requirements.** 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 demonstration of successful certification of these alternative standards in accordance with Article V, Section 1(j).
- 2. Data Breach.** In the event that LEA’s Student Data or Teacher Data maintained by Provider is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and in accordance with applicable law, taking into consideration the legitimate needs of law enforcement and no later than within ten (10) business days following a confirmed data breach. Provider shall follow the following process:
- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “When it Occurred,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
 - b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

- i.** The name and contact information of the reporting LEA subject to this section, when applicable.
- 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.
- v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- vi.** The estimated number of students and teachers affected by the breach, if any, if that information is possible to determine at the time the notice is provided. If not possible at the time of the notice, the Provider will provide the information when available.

Notwithstanding the foregoing, if the security breach notification contains the minimum information described above in Section 2(b), failure of the security breach notification to include the headings as described above shall not be deemed to be a breach by Provider of its obligations hereunder.

- c.** At LEA's discretion, the security breach notification may also include any of the following:
 - i.** Information about what the agency has done to protect individuals whose information has been breached.
 - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d.** Provider agrees to adhere to all requirements in the New Hampshire Data Breach law and in federal law with respect to a data breach related to the Student Data and Teacher Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach as applicable to Provider's role in the data breach.
- e.** 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 of LEA's Student Data, Teacher Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
- f.** If required by applicable federal or state law, Provider shall notify the affected parent, legal guardian or eligible pupil of the data breach, which notice shall include the information required by applicable law.

ARTICLE VI: MISCELLANEOUS

- 1. Term.** The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data or Teacher Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years as long as the Underlying Agreement is in place.
- 2. Termination.** In the event that either party seeks to terminate this DPA, such party may do so by mutual written consent, or with no less than thirty (30) days prior written notice to the other party. The LEA may terminate this DPA and the Underlying Agreement if the Provider breaches any terms of this DPA, but only after (i) the LEA has provided Provider with written notice stating with specificity the nature of the breach, and (ii) the thirty (30) day period following Provider's receipt of the notice has elapsed and Provider has failed to cure or remedy the breach, unless such breach cannot be cured or remedied within thirty (30) days in which case the period for remedy or cure shall be extended for a reasonable time, not to exceed an additional thirty (30) days, provided that Provider is making good faith efforts to address the issue(s) identified in the breach notice. During such notice and cure period LEA shall reasonably cooperate with Provider in trying to resolve any dispute related to the issue(s) identified in the LEA's breach notice.
- 3. Effect of Termination.** If the DPA is terminated, the Provider shall comply with the steps outlined in Article IV, section 5.
- 4. Priority of Agreements.** The parties acknowledge and agree that this DPA amends the Underlying Agreement as of the effective date of this DPA. In the event there is conflict between the terms of the DPA and the Underlying Agreement, the terms of the DPA shall apply and take precedence.
- 5. Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives below.

The designated representative for the Provider for this Agreement is:

Name: Abigail Diaz
Title: Chief Legal Officer
Address: One Tyler Drive, Yarmouth, ME 04096
Telephone
Number: 1-800-772-2260 x4289
Email: Abigail.diaz@tylertech.com

The designated representative for the LEA for this Agreement is:

Name: Gregory Reinert
Title: Director of Technology
Address: SAU 24, 258 Western Ave, Henniker, New Hampshire, 03242

Telephone
Number: (603)428-3269
Email: greg.reinert@sau24.org

6. **Entire Agreement.** This DPA constitutes 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, except the Underlying Agreement which this DPA amends. 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.
7. **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.
8. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF MERRIMACK COUNTY OR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data, Teacher Data, and any portion thereof contained therein, all related or associated institutions or employees who may have access to the Student Data, Teacher Data, and/or any portion thereof.
10. **Waiver.** No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this New Hampshire Student Data Privacy Agreement as of the last day noted below.

HENNIKER – SAU 24

By: *Gregory J Reinert* Date: 2/3/21
Gregory J Reinert (Feb 3, 2021 12:16 EST)

Printed Name: Gregory Reinert Title/Position: Director of Technology

TYLER TECHNOLOGIES, INC.

By: *Andrea Fravert* Date: February 2, 2021

Printed Name: Andrea Fravert Title/Position: Director of Legal Affairs

EXHIBIT “A”

DESCRIPTION OF SERVICES

Infinite Visions, an integrated ERP system that delivers financial, human resources, payroll, and reporting functionality with respect to Teacher Data, as more particularly described in the Underlying Agreement.

EXHIBIT “B”

SCHEDULE OF STUDENT DATA

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

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low-income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
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.	
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

SCHEDULE OF 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	X
	Place of Birth	X
	Social Security Number	X
	Ethnicity or race	X
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	X
	Personal Email	X
	Personal Phone	X
Performance Evaluations	Performance Evaluation Information	X
Schedule	Teacher scheduled courses	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify: Misc. Tracking which is client specific but can include PII such as Driver's License Info	X

Category of Data	Elements	Check if used by your system
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.	
	Other teacher work data - Please specify:	
Education	Course grades from schooling	
	Other transcript data -Please specify: Certification and Licensure Data	X
Other	Please list each additional data element used, stored or collected by your application:	

EXHIBIT “C”

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information (“PII”) from student records or Teacher Data in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider’s specific steps to de-identify the data will depend on the circumstances but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

NIST 800-63-3: Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, Student Data, Teacher Data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address
Unique pupil identifier	
Credit card account number, insurance account number, and financial services account number	
Name of the student's parents or other family members	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student’s Educational Record

Information in the Student’s Email

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 pupil records.

Pupil Generated Content: The term “pupil-generated content” means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

School Official: For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records. The definition of “school official” encompasses the definition of “authorized school personnel” under 603 CMR 23.02.

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, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information, text messages, documents, 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, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of New Hampshire and Federal 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.

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

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Teacher: It includes teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

Teacher Data: For the purposes of this DPA, it applies to teachers, paraprofessionals, principals, school employees, contractors, and other administrators. It includes 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.

Third Party: The term “Third Party” means an entity that is not the provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs Tyler Technologies, Inc. to dispose of data obtained by Company pursuant to the terms of the DPA 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. Timing 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






InfiniteVisions_StaffPII_SAU24

Final Audit Report

2021-02-03

Created:	2021-02-03
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAABAW-mgQQxUehSk8shtzqsgdMSwVc1BqujK

"InfiniteVisions_StaffPII_SAU24" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2021-02-03 - 4:16:29 PM GMT- IP address: 100.1.115.187
-  Document emailed to Gregory J Reinert (greg.reinert@sau24.org) for signature
2021-02-03 - 4:16:51 PM GMT
-  Email viewed by Gregory J Reinert (greg.reinert@sau24.org)
2021-02-03 - 5:15:46 PM GMT- IP address: 69.11.184.74
-  Document e-signed by Gregory J Reinert (greg.reinert@sau24.org)
Signature Date: 2021-02-03 - 5:16:21 PM GMT - Time Source: server- IP address: 69.11.184.74
-  Agreement completed.
2021-02-03 - 5:16:21 PM GMT