AMENDMENT

This amendment ("Amendment") is effective as of the date of signature of the last party to sign as indicated below ("Amendment Effective Date"), by and between Tyler Technologies, Inc. with offices at One Tyler Drive, Yarmouth, Maine 04096 ("Tyler") and the Burnt Hills-Ballston Lake Central School District, with offices at 88 Lakehill Road, Ballston Lake, New York 12027 ("Client").

WHEREAS, Tyler and the Client are parties to an agreement dated November 18, 2022 ("Agreement"); and

WHEREAS, Tyler and Client desire to amend the terms of the Agreement as provided herein.

NOW THEREFORE, in consideration of the mutual promises hereinafter contained, Tyler and the Client agree as follows:

1. The student data privacy addendum attached hereto as Amendment Exhibit 1 hereby replaces existing Exhibit F of the Agreement.

2. This Amendment shall be governed by and construed in accordance with the terms and conditions of the Agreement.

3. Except as expressly indicated in this Amendment, all other terms and conditions of the Agreement shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment as of the dates set forth below.

Tyler Technologies, Inc.

By: _____

Name: Theodore J. Thien

Title: VP and General Manager, Transportation

Date: 04/27/2023

Burnt Hills-Ballston Lake Central School District

By: _____ Patrick McGrath (Apr 28, 2023 10:21 EDT)

Name: Patrick M. McGrath, Jr., Ph.D.

Title: Superintendent of Schools

Date: 04/28/2023

Exhibit F

BURNT HILLS-BALLSTON LAKE BOLIVAR-RICHBURG CENTRAL SCHOOL DISTRICT

and

Tyler Technologies, Inc.

This Data Privacy Addendum ("DPA") is by and between the Burnt Hills-Ballston Lake Central School District ("EA"), an Educational Agency, and Tyler Technologies, Inc. ("Contractor"), collectively, the "Parties," and supplements and is attached as an exhibit to the November 18, 2022 Software as a Service Agreement between the Parties.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or by or to a person not authorized to acquire, access, use, or receive it.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, 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.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal 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.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

In order for Contractor to provide certain technologies on one or more of Contractor's digital platforms ("Services") to the EA pursuant to a Software as a Service Agreement to which this addendum is attached as an exhibit ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements

of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York State and federal laws, rules, and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate the applicable New York laws referenced in Section 1 above.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State and federal laws and regulations. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy; Ed Law Section 2-d and the applicable parts of Part 121 of the Regulations of the Commissioner of Education.

5. **Right of Review and Audit.**
   Upon request by the EA, Contractor shall share with the EA with a summary of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors**.

(a) Contractor shall limit access to PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the access to PII shall be limited to the extent necessary to provide such Services. Contractor shall require that all such employees and subcontractors comply with data privacy terms consistent with those required of Contractor in this DPA.

(b) Contractor acknowledges that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point Contractor becomes aware that a subcontractor has failed to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is Data Breach in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Except for subcontractors engaged to provide Services by Contractor, Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII to the EA in a standard file format agreed to by the Parties. If agreed to by the EA, the Contractor can assist and provide instructions to the EA to allow the EA to extract its PII using the standard functionality of Contractor's products.

(b) Contractor agrees to destroy all PII when the purpose that necessitated its receipt by Contractor has been completed, no later than sixty (60) days after termination or expiration of the initial Service Agreement or the termination or expiration of any subsequent Service Agreement as agreed to by the Parties; provided, however that Contractor shall dispose of PII in its data backups pursuant to Contractor's then-current data retention and destruction policy and in no event later than thirteen (13) months after the expiration of the Services Agreement and provided further that Contractor may retain PII for so long as necessary for litigation purposes. Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction. Contractor may maintain de-identified data that will no longer meet the definition of PII as set forth in this DPA. Such information will be aggregate data to be used by the Contractor for research and development purposes only.

(c) Upon written request from EA, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data

and not to transfer de-identified data to any party except for third parties providing services to the Contractor and as agreed to by the EA.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be made by the most expedient way possible and may be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), Contractor's regular client communication channels, or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph may be provided to the EA at the following address:

Name: Burnt Hills-Ballston Lake Central School District

Title: General Counsel

Address: 88 Lakehill Road

City, State, Zip: Ballston Lake, New York 12027

Email: **pjfv@girvinlaw.com**

13. **Cooperation with Investigations.**
Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**
Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.
The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for assistance, such as instructions, to access to Student Data using the standard product functionality so the EA can facilitate such review and corrections by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.
As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	**CONTRACTOR**
BY: ***[Signature]*** Patrick McGrath (Apr 28, 2023 10:21 EDT)	BY: ***[Signature]***
[Printed Name] Patrick M. McGrath, Jr., Ph.D.	***[Printed Name]*** Theodore J. Thien
[Title] Superintendent of Schools	**[Title]** VP and General Manager, Transportation
Date: 04/28/2023	Date: 04/27/2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

The Burnt Hills-Ballston Lake Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII)[2] in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Burnt Hills-Ballston Lake Central School District establishes the following parental bill of rights:

 Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law. Specifically, parents are assured:

- that it is the district's policy to disclose personally identifiable information from student records, without consent, to other *school officials* within the district whom the district has determined to have *legitimate educational interests*. The notice will define 'school official' and 'legitimate educational interest.'

  District policy P5500 provides the following definitions:

  - *Legitimate Educational Interest:* a school official has a legitimate educational interest if they need to review a student's record in order to fulfill their professional responsibilities;
  - *School Official*: a person who has a legitimate educational interest in a student record who is employed by the district as an administrator, supervisor, instructor or support staff member (including health or medical staff and law enforcement unit personnel); a member of the Board of Education; a person or company with whom the district has contracted to perform a special task (such as attorney, auditor, medical consultant or therapist); or a parent or student serving on an official committee, such as disciplinary or grievance committee, or assisting another school official performing their tasks.

- that, upon request, the district will disclose education records without consent to officials of another school district in which a student seeks to or intends to enroll or is actually enrolled.
- that personally identifiable information will be released to third party authorized representatives for the purposes of educational program audit, evaluation, enforcement or compliance purposes.
- that the district, at its discretion, releases directory information (see P5500) without prior consent, unless the parent/guardian or eligible student has exercised their right to prohibit release of the information without prior written consent. The district will not sell directory information.
- that, upon request, the district will disclose a high school student's name, address and telephone number to military recruiters and institutions of higher learning unless the parent or secondary school student exercises their right to prohibit release of the information without prior written consent.
- that the district will provide information as a supplement to the 'Parents' Bill of Rights' about third parties with which the district contracts that use or have access to personally identifiable student data.
- that a student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any a third party contractor. The district will not sell student personally identifiable information. The district will not release it for

marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

- Parents[1] have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see AR-5500); Parents have the right to request that records be amended to ensure that they are not inaccurate, misleading, or otherwise in violation of the student's privacy rights;

- State and federal laws[3], such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, and the Individuals with Disabilities Education Act protect the confidentiality of students' personally identifiable information. Specifically,

    - Parents have the right to consent to disclosure of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent; and
    - Parents have the right to file a complaint with the United States Department of Education alleging failure of the district to comply with FERPA and its regulations; and/or file a complaint regarding a possible data breach by a third party contractor with the district and/or the New York State Education Department's Chief Privacy Officer for failure to comply with state law.

- Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov.data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the district's Data Protection Officer. Complaints can also be directed to the New York State Education Department online at http://nysed.gov.data-privacy-security, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII

- In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the district's Data Protection Officer (see www.bhbl.org).

- In the course of complying with its obligations under the law and providing educational services to District residents, the Burnt Hills-Ballston Lake Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation. For each contract or other written agreement that the District enters into with a third-party

contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included in the contract and published on the District Web Page:

- The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor wilt disclose the student data or teacher or principal data, if any, will abide by atl applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- Address how the data will be protected using encryption while in motion and at rest.

 A parent or eligible student may challenge the accuracy of student data concerning that student or eligible student pursuant to the procedures provided for amendment of educational records under the Family Educational Rights and Privacy Act (FERPA).

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter, and personal characteristics or information as such term is used under section 20 of the United States Code, section 1400 et seq., and implementing regulations at section 34 Code of Federal Regulations at 300.32.

[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

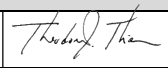
CONTRACTOR	
[Signature]	
[Printed Name]	Theodore J. Thien
[Title]	VP and General Manager, Transportation
Date:	04/27/2023

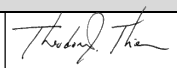
EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	**Tyler Technologies, Inc.**
Description of the purpose(s) for which Contractor will receive/access PII	Protected Data will be used only as necessary for Contractor to perform the services in the Service Agreement, and disclosed to only its authorized officers, employees, subcontractors and third-party service providers with whom it shares Protected Data necessary to perform the services.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date November 18, 2022 Contract End Date As stated in the Services Agreement
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☑ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Contractor will transfer PII to the EA, or upon consent of the EA, assist the EA in retrieving securely transfer data utilizing the standard functionality of Contractor's services, where applicable, no less than 15 days prior to expiration or termination of the Service Agreement. • Securely delete and destroy data within sixty (60) days after expiration or termination of the Service Agreement, provided, however that Contractor shall dispose of PII in its data backups pursuant to Contractor's then-current data retention and destruction policy

	and in no event later than thirteen (13) months after the expiration of the Services Agreement and provided further that Contractor may retain PII for so long as necessary for litigation purposes.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. Parents reaching out to the Contractor will be referred to the EA. The EA will have access for review or correction through standard functionality of Contractor's services. Contractor agrees to assist the EA as may be necessary and to facilitate such corrections, such as with instructions, within 30 calendar days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Theodore J. Thien
[Title]	VP and General Manager, Transportation
Date:	04/27/2023

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state**. While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	During the term of the Agreement, Tyler will use reasonable, industry standard and technically feasible internal controls to address its compliance obligations under federal and state data security and privacy laws, including NY Education Privacy Laws, as they apply to Tyler's performance of services under the Agreement. Tyler will use reasonable, industry standard and technically feasible internal controls to address compliance with those provisions of Client's data security and privacy policy that apply to Tyler's performance of services under the Agreement, to the extent Client's data security and privacy policy has been provided by Client and agreed to by Tyler in writing as of the Effective Date, and thereafter only as mutually agreed to by Client and Tyler.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Tyler will protect PII that it receives under the Agreement using industry standard security measures utilizing the following: (i) administrative controls (for example, Tyler organizes itself to emphasize security and ensure human resource processes are in place to help facilitate security; (ii) physical controls (for example, Tyler invests in secure data centers and associated practices in support of its hosted solutions); and (iii) technical controls (for example, Tyler hosted solutions are secured through a layered series of barriers and

		monitoring tools that are designed to detect and defeat unauthorized attempts to reach client hosted data).
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All Tyler employees who have access to Student Data, or Teacher or Principal Data under the Agreement have or will receive, prior to obtaining access to said data, Tyler's standard information security and privacy awareness training. Additionally, all Tyler employees sign confidentiality agreements which extend to Student Data and Teacher and Principal Data.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Tyler subcontractors or other third party authorized persons or entities, if any, to whom Tyler discloses Student Data, or Teacher or Principal Data, must agree to comply with data protection and security requirements as required by applicable federal and state laws and regulations.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Tyler will manage data security and privacy incidents that implicate Personally Identifiable Information in Tyler's possession or control in accordance with the applicable requirements of Part 121.10 of the New York Education Privacy Laws.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon the expiration of the term of the Agreement, Tyler will, at Client's election, either (i) return all Student Data, Teacher or Principal Data which is in Tyler's possession, to the Client in an industry standard data format, or as otherwise agreed to by Tyler and Client; or (ii) destroy all Student Data, Teacher or Principal Data, in Tyler's possession to the fullest extent commercially feasible, as soon as practicable upon expiration of the Agreement or as otherwise required by applicable law. To the extent that destruction of all Student Data, and

		Teacher or Principal Data, is infeasible Tyler's obligations under this Plan with respect to such Student Data, and Teacher or Principal Data, will continue for as long as Tyler retains such data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon the expiration of the term of the Agreement, Tyler will, at Client's election, either (i) return all Student Data, Teacher or Principal Data which is in Tyler's possession, to the Client in an industry standard data format, or as otherwise agreed to by Tyler and Client; or (ii) destroy all Student Data, Teacher or Principal Data, in Tyler's possession to the fullest extent commercially feasible, as soon as practicable upon expiration of the Agreement or as otherwise required by applicable law. To the extent that destruction of all Student Data, and Teacher or Principal Data, is infeasible Tyler's obligations under this Plan with respect to such Student Data, and Teacher or Principal Data, will continue for as long as Tyler retains such data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	During the term of the Agreement, Tyler will use reasonable, industry standard and technically feasible internal controls to address its compliance obligations under federal and state data security and privacy laws, including NY Education Privacy Laws, as they apply to Tyler's performance of services under the Agreement. Tyler will use reasonable, industry standard and technically feasible internal controls to address compliance with those provisions of Client's data security and privacy policy that apply to Tyler's performance of services under the Agreement, to the extent Client's data security and privacy policy has been provided by Client and agreed to by Tyler in writing as of the Effective Date, and thereafter

		only as mutually agreed to by Client and Tyler.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

Tyler Data Security and Privacy Plan For New York

Tyler sets forth the following Data Security and Privacy Plan with respect to Tyler Software and services ("Plan") in accordance with the requirements of New York Education Law §2-d and the implementing regulations set forth in Part 121 of the Regulations of the Commissioner of Education ("NY Education Privacy Laws"). Capitalized but undefined terms shall have the meaning attributed to them in the NY Education Privacy Laws.

The Plan amends the Agreement and is incorporated into the Agreement by reference.

SECTION A

Bill of Rights for Data Privacy and Security

Client has provided to Tyler, and Tyler has reviewed, Client's Parents Bill of Rights for data privacy and security ("Bill of Rights") in effect as of the Effective Date of the Agreement, and agrees to incorporate the Bill of Rights by reference in its entirety, as if fully set forth herein. Any changes made by Client to its Bill of Rights after the Effective Date shall not be incorporated into the Agreement unless agreed to by Tyler in writing. Client and Tyler agree to cooperate in good faith to address each party's respective obligations under applicable data privacy and security requirements.

Additionally, the following information is provided to assist Client with developing the supplemental information required by Part 121.3(c) of the NY Education Privacy Laws:

1. Student Data, or Teacher or Principal Data, will be used and disclosed by Tyler solely for providing the Tyler Software and Tyler services purchased by Client through its Agreement with Tyler. Nothing in this Plan shall be construed to apply to Third Party Products and Third Party Services purchased by Client pursuant to the Agreement.
2. Tyler subcontractors or other third party authorized persons or entities, if any, to whom Tyler discloses Student Data, or Teacher or Principal Data, must agree to comply with data protection and security requirements as required by applicable federal and state laws and regulations.
3. Upon the expiration of the term of the Agreement, Tyler will, at Client's election, either (i) return all Student Data, Teacher or Principal Data which is in Tyler's possession, to the Client in an industry standard data format, or as otherwise agreed to by Tyler and Client; or (ii) destroy all Student Data, Teacher or Principal Data, in Tyler's possession to the fullest extent commercially feasible, as soon as practicable upon expiration of the Agreement or as otherwise required by applicable law. To the extent that destruction of all Student Data, and Teacher or Principal Data, is infeasible Tyler's obligations under this Plan with respect to such Student Data, and Teacher or Principal Data, will continue for as long as Tyler retains such data.
4. Client shall be solely responsible for addressing challenges to the accuracy of Student Data, or Teacher or Principal Data, processed by Tyler pursuant to the Agreement, or any other inquiry made by a third party with respect to said data. In the event that Tyler receives a third party request for access to Student Data, or Teacher or Principal Data, whether such request is made in accordance with the NY Education Laws or other applicable

Federal or State law or regulation, Tyler will promptly inform Client of such request in writing, if allowed by law or judicial and/or administrative order.

5. If Tyler is hosting Student Data, or Teacher or Principal Data, such hosted data will be stored in a secure hosting facility in the United States. Tyler maintains industry standard intrusion detection and prevention systems to monitor malicious activity attempting to access hosted data. Tyler data centers are accessible only by authorized personnel with a unique key entry. Entry attempts to the data center are regularly audited by internal staff and external auditors to ensure no unauthorized access. In the event a third party will be hosting said data, Tyler will ensure that said third party has security protections equivalent or more stringent than those set forth herein.
6. Student Data or Teacher or Principal Data transmitted between Client workstations and the Tyler or third party hosting center will be encrypted using industry standard methods for data in transit, as applicable. Student Data or Teacher or Principal Data hosted in a Tyler or third party data center will be encrypted using industry standard methods for data at rest, as applicable.

SECTION B

Data Security and Privacy Plan

As required by Part 121.6(a) of the NY Education Privacy Laws, Tyler hereby identifies and incorporates into this Plan the following elements:

1. During the term of the Agreement, Tyler will use reasonable, industry standard and technically feasible internal controls to address its compliance obligations under federal and state data security and privacy laws, including NY Education Privacy Laws, as they apply to Tyler's performance of services under the Agreement. Additionally, Tyler will use reasonable, industry standard and technically feasible internal controls to address compliance with those provisions of Client's data security and privacy policy that apply to Tyler's performance of services under the Agreement, to the extent Client's data security and privacy policy has been provided by Client and agreed to by Tyler in writing as of the Effective Date, and thereafter only as mutually agreed to by Client and Tyler.
2. Tyler will protect Personally Identifiable Information that it receives under the Agreement using industry standard security measures utilizing the following: (i) administrative controls (for example, Tyler organizes itself to emphasize security and ensure human resource processes are in place to help facilitate security; (ii) physical controls (for example, Tyler invests in secure data centers and associated practices in support of its hosted solutions); and (iii) technical controls (for example, Tyler hosted solutions are secured through a layered series of barriers and monitoring tools that are designed to detect and defeat unauthorized attempts to reach client hosted data).
3. Tyler has provided all information required of it by Part 121.3(c) of the NY Education Privacy Laws in Section A of this Plan, and will comply with the applicable requirements of the supplemental information, as required and to the extent not inconsistent with its obligations under applicable law.
4. All Tyler employees who have access to Student Data, or Teacher or Principal Data under the Agreement have or will receive, prior to obtaining access to said data, Tyler's standard information security and privacy awareness training. Additionally, all Tyler employees sign confidentiality agreements which extend to Student Data and Teacher and Principal Data.
5. Tyler will manage data security and privacy incidents that implicate Personally Identifiable Information in Tyler's possession or control in accordance with the applicable requirements of Part 121.10 of the New York Education Privacy Laws.
6. Tyler will comply with applicable requirements of Part 121.9 of the NY Education Privacy Laws in its performance of the Agreement.

7. Tyler will comply with applicable requirements of Part 121.10 of the NY Education Privacy Laws in notifying Client in the event of any Breach or Unauthorized Release of Client's Personally Identifiable Information in Tyler's possession or control.

Burnt Hills-Ballston Lake CSD, NY DPA Amendment 042723

Final Audit Report 2023-04-28

Created:	2023-04-27
By:	Tracey Stegemann (tracey.stegemann@tylertech.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAfYvpf4IbpFogjKVlijQZ6Cmu2CCuybj5

"Burnt Hills-Ballston Lake CSD, NY DPA Amendment 042723" History

Document created by Tracey Stegemann (tracey.stegemann@tylertech.com)
2023-04-27 - 2:12:47 PM GMT- IP address: 98.11.230.241

Document emailed to Theodore Thien (ted.thien@tylertech.com) for signature
2023-04-27 - 2:16:49 PM GMT

Email viewed by Theodore Thien (ted.thien@tylertech.com)
2023-04-28 - 1:42:39 AM GMT- IP address: 100.4.189.45

Document e-signed by Theodore Thien (ted.thien@tylertech.com)
Signature Date: 2023-04-28 - 1:43:16 AM GMT - Time Source: server- IP address: 100.4.189.45

Document emailed to Patrick McGrath (pmcgrath@bhbl.org) for signature
2023-04-28 - 1:43:19 AM GMT

Email viewed by Patrick McGrath (pmcgrath@bhbl.org)
2023-04-28 - 2:19:51 PM GMT- IP address: 163.153.222.100

Document e-signed by Patrick McGrath (pmcgrath@bhbl.org)
Signature Date: 2023-04-28 - 2:21:00 PM GMT - Time Source: server- IP address: 163.153.222.100

Agreement completed.
2023-04-28 - 2:21:00 PM GMT