



## 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 Shenendehowa Central School District, with offices at 970 Route 146, Clifton Park, New York 12065 ("Client").

WHEREAS, Tyler and the Client are parties to an agreement dated May 23, 2012 ("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 Data Security and Privacy Plan attached hereto as Exhibit 1 is hereby made a part 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.

Shenendehowa Central School District

By: Robert Kennedy-Jensen

By: Rebecca Carman

Name: Robert Kennedy-Jensen

Name: Rebecca Carman

Title: Group General Counsel

Title: DPO

Date: August 22, 2022

Date: 8/23/22



## Exhibit 1

### Data Security and Privacy Plan

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 set forth in Schedule A to this Data Security and Privacy Plan. 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.

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, place of birth, social security number, biometric record & mother's maiden name, which when linked to or combined with other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or any information requested by a person if the educational agency or institution reasonably believes that person knows the identity of the student to whom the education record relate
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, 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); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed.  
(i) Complaints should be submitted to the Shenendehowa Central School District, Director of Policy & Community Development/Data Protection Officer, 5 Chelsea Place, Clifton Park, NY 12065. (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Tyler Technologies, Inc. – Acknowledgment of Having Reviewed the Above Bill of Rights for Data Privacy and Security	
[Signature]	<i>Robert Kennedy-Jensen</i>
[Printed Name]	Robert Kennedy-Jensen
[Title]	Group General Counsel
Date:	August 22, 2022