

**NEW HAMPSHIRE STUDENT DATA PRIVACY ACKNOWLEDGEMENT**

**Inter-Lakes School District**

**and**

**Tallo, Inc.**

This New Hampshire Student Data Privacy Acknowledgement (“DPA”) is entered into by and between the school district, Inter-Lakes School District (hereinafter referred to as “LEA”) and Tallo, Inc. (hereinafter referred to as “Provider”) on 12/9/2021. The Parties agree to the terms as stated herein.

1. **Purpose of DPA.** The purpose of this DPA is to identify the duties and responsibilities that LEA acknowledges and agrees Provider, and which Provider acknowledges and agrees it, will undertake to help protect Student Data (as defined in Exhibit “B”) transmitted to Provider by students using the LEA’s network and with the support of the LEA pursuant to Exhibit “A”.
2. **DPA Definitions.** The definitions for terms used in this DPA are found in Exhibit “B”.
3. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA or the party who provided such data (such as the student or parent). The LEA and Provider agree that students independently may enter into a separate contractual relationship with Provider, involving the provision of Student Data by students to Provider and uses of such data provided beyond this DPA. If an individual student forms a direct relationship with the Provider outside of the DPA, neither this DPA nor its restrictions will apply to that individual student data that the student provides directly to the Provider. The Provider agrees that the LEA shall not have responsibility or liability for any terms and conditions in that contractual relationship.
4. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRa, 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 applicable privacy statutes. The LEA agrees that it will obtain the written consent of the parent/guardian or eligible student, compliant with such statutes, to authorize Provider to release Student Data within its closed network to authorized licensees for the intended purposes of Provider’s Services pursuant to an authorization form appended hereto as Exhibit “D.”
5. **Reasonable Precautions.** LEA shall take no less than reasonable precautions to secure usernames, passwords, and any other means of gaining access to Student Data.
6. **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.
7. **Privacy Compliance.** The Provider shall comply with all applicable New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRa, 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.
8. **Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than as authorized by the written consent of the parent/guardian or eligible student or permitted by applicable New Hampshire and Federal laws and regulations pertaining to data privacy and security.

- 9. Employee/Subprocessor Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under this DPA. Provider will ensure that Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.
- 10. No Disclosure.** The Provider will not use, disclose, compile, transfer, sell the Student 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, transfer or sell the Student Data and/or any portion thereof without the express written consent of the LEA (authorizing Provider to disclose such data as a “school official” within the meaning of FERPA), without express written consent from the student who is over eighteen (18) and/or parent/legal guardian, through a separate agreement directly between the Provider and the student (such separate agreement does not impact the Provider’s obligations to maintain and process Student Data provided pursuant to this DPA in accordance with this DPA) or without a court order or lawfully issued subpoena. De-identified information, as defined in Exhibit “B”, may be used by the Provider for any lawful purpose(s), including development, research, and improvement of educational sites, services,. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless that party agrees in writing not to attempt re-identification.
- 11. Advertising Prohibition.** Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) for any commercial purpose; and (d) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA.
- 12. Disposition of Data.** Provider shall delete all personally identifiable data obtained from a student and/or parent when requested by the parent/guardian or eligible student within sixty (60) days of the request. 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 to the extent necessary for any audit, to comply with legal process, including subpoenas, court orders or other compulsory disclosures, or to respond to claims of a violation of the rights of third parties. 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.
- 13. Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below.
- a. Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data.
  - b. Destruction of Data.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA as directed by the student to whom the Student Data relates.
  - c. Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data.

- d. Employee Training.** The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider’s business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hackers, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits.
- e. Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer (“SSL”), or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption.
- f. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- g. Audits.** No more than once a year, except in the case of a verified breach and upon written request of the LEA, the Provider will provide to the LEA a third party certification of its security and privacy measures. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider’s facilities, staff, agents and Student Data provided pursuant to this Agreement and all records pertaining to the Provider, LEA and delivery of Services by the Provider.
- h. New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from “the Minimum Standards for Privacy and Security of Student and Employee Data” from the New Hampshire Department of Education. Specifically, the Provider agrees to:

  - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

- (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
- (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
- (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
- (9) Enforce a minimum password complexity and change of characters when new passwords are created;
- (10) Perform maintenance on organizational systems;
- (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1;
- (13) Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;
- (14) Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- (15) Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas;
- (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22) Monitor system security alerts and advisories and take action in response; and

(23) Update malicious code protection mechanisms when new releases are available.

- i. 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, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- j. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to answer questions of the LEA at reasonable times about the written incident response plan.

**14. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and no later than within ten (10) days of the incident. 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:

- (1) The name and contact information of the reporting LEA subject to this section.
- (2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- (3) 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.
- (4) 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.
- (5) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (6) The estimated number of students and teachers affected by the breach, if any.

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, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such 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, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

**15. Priority of Agreements.** This DPA shall govern the treatment of Student Data provided to Provider pursuant to this DPA in order to comply with the privacy protections, including, where applicable, those found in FERPA, IDEA, COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

**16. 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 [COUNTY OF LEA] COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

**17. Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA and does not cure the breach within thirty (30) days of receipt of written notice.

**18. Term.** The parties shall be bound by this DPA for three (3) years.

**19. Waiver.** No delay or omission of either party to exercise any right hereunder shall be construed as a waiver of any such right and the parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**20.** Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit “C”), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

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

**INTER-LAKES SCHOOL DISTRICT**

By: *Mark J Parsons* Date: 12/9/2021  
Mark J Parsons (Dec 9, 2021 13:50 EST)

Printed Name: Mark J Parsons Title/Position: CIO

**TALLO, INC.**

By: *John J. Drozdowski* Date: 12/09/2021  
John J. Drozdowski (Dec 9, 2021 13:39 EST)

Printed Name: John J. Drozdowski Title/Position: CFO



## **EXHIBIT “A”**

### DESCRIPTION OF SERVICES

**Tallo**, an online platform that enables students to showcase their accomplishments in areas such as science, mathematics, and technology and to connect with colleges, universities and potential employers. The Tallo app assists students in designing a career pathway, educators in recruiting top talent to their schools, and employers in developing a stable, continuous talent pipeline. Through these connections within Tallo’s closed network, students are connected with opportunities and resources of potential interest and relevance such as scholarships, financial aid, industry and organizational competitions, apprenticeships, internships, mentorships and training programs.

## EXHIBIT “B”

### DEFINITIONS

**De-Identifiable Information (DII):** De-Identification refers to the process by which an entity removes or obscures any Personally Identifiable Information (“PII”) from student records 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.

**Personally Identifiable Information (PII):** The terms “Personally Identifiable Information” or “PII” shall include information that identifies an individual person, including but not limited to, the following:

- |   |                             |
|---|-----------------------------|
| First Name  | Home Address                |
| Last Name   | Email Address               |
| Telephone Number  | Individual Test Results     |
| Discipline Records  | Juvenile Dependency Records |
| Unique Special Education Data   | Evaluations                 |
| Transcript/Grades   | Medical Records             |
| Criminal Records  | Social Security Number      |
| Health Records  | Credit card account number  |
| Biometric Information   | Financial Account Number    |
| Student Identifiers   | Disabilities                |
| Insurance Account Number  |                             |
| 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                                       |                             |
| Socioeconomic Information   | Food Purchases              |
| Political Affiliations  | Religious Information       |
| Photos  | Voice Recordings            |
| Videos  |                             |

**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

**Pupil Records:** Means both of the following: Any information that directly relates to a pupil that is maintained and provided by LEA and shall include such other information as expressly prescribed by the applicable Federal or New Hampshire laws or regulations.

**Student Data:** Student Data includes any data that is descriptive of the student. It includes the categories of information in PII. 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 include or constitute (i) that information that has been anonymized or de-identified, (ii) anonymous usage data regarding a student's use of Provider's services, (iii) students' PII that has been furnished to Provider independent of the Services or (iv) PII that, at the election of the parent or student, remains with Provider following a student's graduation or disenrollment.

**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. the 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.

**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.

**Third Party:** The term "Third Party" means an entity that is not the Provider or LEA or one of their respective affiliates or subsidiaries.

**EXHIBIT “D”**

**PARENTAL RELEASE**

**Informed Consent and Release**

I, the undersigned parent/legal guardian, hereby understand that [School District] is utilizing Tallo, an online application. I also understand that as part of this activity my child will be providing categories of information as outlined the District’s DPA with Tallo in order to use this online application.

I understand that to the extent that either I or my child are provided with or create a password for the use of this site, that my child and I can help protect against unauthorized access to my child’s account and personal information by appropriately protecting and limiting access to this password and appropriately logging off of the account when finished. I hereby acknowledge that my child’s Student Data that are posted on or through this website shall be managed and controlled by Tallo in accordance with its Terms of Use and Privacy Policy. I further acknowledge that my child and I have read Tallo’s [Terms of Use](#) and [Privacy Policy](#), true copies which are linked to this informed consent and release.

By entering into this informed consent and release and granting the permission as stated herein, I am expressly authorizing my child to participate, use and submit Student Data to Tallo.

I also am expressly authorizing Tallo to share my child’s Student Data within Tallo’s closed network of opportunities and resources of potential interest and relevance such as scholarships, financial aid, industry and organizational competitions, apprenticeships, internships, mentorships and training programs.

I further understand that Tallo will not delete or destroy my child’s Student Data upon the District’s request or upon my child’s graduation or disenrollment from the District. If I would like to request deletion of my child’s data, I need to contact Tallo directly.

I have read this Informed Consent and Release and understand its terms. I sign it voluntarily and with full knowledge of its significance.

Child’s Name: \_\_\_\_\_ Grade: \_\_\_\_\_

Child’s Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Parent/Guardian’s Name: \_\_\_\_\_

Parent/Guardian’s Signature: \_\_\_\_\_ Date: \_\_\_\_\_









# New Hampshire DPA (Final (1))

Final Audit Report

2021-12-09

Created:	2021-12-07
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA4bRNE0T_IQ2AJrUrsfZcumiRx0dDuODr

## "New Hampshire DPA (Final (1))" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2021-12-07 - 8:32:48 PM GMT- IP address: 66.153.170.85
-  Document emailed to John J. Drozdowski (mhoffman@tuckerlaw.com) for signature  
2021-12-07 - 8:34:14 PM GMT
-  Email viewed by John J. Drozdowski (mhoffman@tuckerlaw.com)  
2021-12-09 - 4:57:01 PM GMT- IP address: 18.206.199.142
-  Document e-signed by John J. Drozdowski (mhoffman@tuckerlaw.com)  
Signature Date: 2021-12-09 - 6:39:17 PM GMT - Time Source: server- IP address: 73.131.154.124
-  Document emailed to Mark J Parsons (mark.parsons@interlakes.org) for signature  
2021-12-09 - 6:39:18 PM GMT
-  Email viewed by Mark J Parsons (mark.parsons@interlakes.org)  
2021-12-09 - 6:47:57 PM GMT- IP address: 66.102.8.67
-  Document e-signed by Mark J Parsons (mark.parsons@interlakes.org)  
Signature Date: 2021-12-09 - 6:50:19 PM GMT - Time Source: server- IP address: 216.107.203.2
-  Agreement completed.  
2021-12-09 - 6:50:19 PM GMT