

DATA SHARING AND PRIVACY AGREEMENT

BETWEEN

Pioneer Central School

AND

SLP Toolkit, LLC

This Data Sharing and Privacy Agreement ("DSPA") is made and entered into as of the date signed below, by and between Pioneer Central School (the "Organization"), whose principal place of business is 12145 County Line Road, Yorshire, and SLP Toolkit, LLC ("SLP Toolkit"), whose principal place of business is 136 W. Main St. Suite 101 Mesa, Arizona 85201 (collectively the "Parties"). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, SLP Toolkit has agreed to provide the Organization with access to online software; and

WHEREAS, the Organization has purchased one or more SLP Toolkit accounts and has control over the data associated with these accounts; and

WHEREAS, the Organization may provide data that is covered by a number of federal and local laws, among them, the Family Educational Rights and Privacy Act ("FERPA"); and

WHEREAS, the data transferred from the Organization and/or stored by SLP Toolkit when providing access to online software, is also subject to those privacy laws; and

WHEREAS, the Parties wish to enter into this DSPA to ensure that accessing and/or transferring of data complies with the requirements of the privacy laws referenced above and to establish required procedures and duties; and

NOW THEREFORE, for good and valuable consideration, the Parties agree as described in the following sections.

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DSPA.** For SLP Toolkit to provide services to the Organization, it may become necessary for the Organization to share certain data related to the Organization's students, employees, business practices, and/or intellectual property. This DSPA describes the responsibilities of the Organization and of SLP Toolkit with respect to the data and services provided.
2. **Nature of Services Provided.** SLP Toolkit has agreed to provide the following digital educational services ("Services") described below:

Access to online software which assists faculty and staff in the efficient and effective management of students, including scheduling, assessment, progress monitoring, and related data collection throughout the duration of their IEP's. As part of the Services, we send emails to our users in the following categories. Users may opt out of these emails at any time.

- Onboarding. emails such as "getting started" and other helpful information to ensure district users get the most out of the software.
- Engagement. emails to encourage continued use of the software so that the district gets the most value out of the licenses purchased.
- Professional development. emails promoting opportunities for CEUs & online conferences focused on helping our users become better SLPs.
- Reporting. emails concerning user activities associated with a district account may be sent automatically or by request to District administrators for management purposes.

SLP Toolkit may use aggregate data for the purposes of development, research, and improvement of the Services offered. Provider agrees not to transmit (or sell) aggregate data to any 3rd party, except as necessary to fulfill the Services provided.

3. **Data to Be Provided.** In order to perform the Services described in the DSPA, Organization will likely provide, among other data, the categories of data described below.

Name, IEP Date, Eval Date, School, IEP Service Time, Teacher, Grade level, Date of Birth, or other related information at the discretion of the SLP

4. **Order of Precedence.** In the event of a conflict or inconsistency between this DSPA and any other stated or agreed upon policies, terms, or conditions, this DSPA takes precedence and supersedes all other past agreements between the Organization and SLP Toolkit.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Data Property of Organization.** All educational information, personally identifiable information, and/or directory information for students ("Student Data") transmitted from the Organization to SLP Toolkit pursuant to the DSPA is and will continue to be the property of and under the control of the Organization. SLP Toolkit further acknowledges and agrees that all copies of such Student Data transmitted to SLP Toolkit, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DSPA in the same manner as the original Student Data. The Parties agree that as between them all rights, including all intellectual property rights in and to Student Data contemplated per the DSPA shall remain the exclusive property of the Organization.

For the purposes of FERPA and Pursuant to 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii), SLP Toolkit will provide the specified services the Organization could otherwise use its employees to perform. SLP Toolkit agrees that for purposes of this DSPA, it will be designated a "School Official," under the control and direction of the Organization as it pertains to the use of data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. SLP Toolkit agrees to abide by FERPA and related state statutes while performing the Services for the Organization.

2. **No Unauthorized Use or Disclosure.** SLP Toolkit shall not use Student Data for any purpose other than as explicitly specified in the DSPA. SLP Toolkit will not use, disclose, compile, transfer, or 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, except as may be required in connection with providing the Services. SLP Toolkit shall not make any re-disclosure of any Student Data, including metadata, persistent unique identifiers, or other non-public information or PII, without the express written consent of the Organization.
3. **Data Property of SLP Toolkit.** All content generated by SLP Toolkit for use in the app ("App Content") is owned by SLP Toolkit. App Content is not to be distributed to any 3rd party or used for anything other than the intended purposes within the applications.
4. **Third Party Request.** In the event that a parent of a student or other individual contacts SLP Toolkit to review any Student Data, SLP Toolkit shall refer the parent or individual to the Organization, who will follow the necessary and proper procedures regarding the

requested information. Should a third party, including law enforcement and government entities, contact SLP Toolkit with a request for data held by SLP Toolkit pursuant to the Services, SLP Toolkit shall redirect the third party to request the data directly from the Organization. SLP Toolkit shall notify the Organization in advance of a compelled disclosure to a third party.

5. **Subprocessors.** SLP Toolkit shall enter into written agreements with all subprocessors performing functions pursuant to the DSPA, whereby the subprocessors agree to protect Student Data in a manner consistent with the terms of this DSPA.

ARTICLE III: DUTIES OF Organization

1. **Provide Data In Compliance With State and Federal Law.** The Organization shall allow SLP Toolkit access to data necessary to perform the Services, and pursuant to the terms of this DSPA, and in compliance with FERPA and all other applicable privacy statutes.
2. **Annual Notification of Rights.** If the Organization has a policy of disclosing education records under FERPA, the Organization shall include a specification of criteria for determining what constitutes a legitimate educational interest in its annual notification of rights, and determine whether SLP Toolkit qualifies as a school official.
3. **Reasonable Precautions.** The Organization shall take reasonable precautions to secure user names, passwords, and any other means of gaining access to the Services and hosted data.
4. **Unauthorized Access Notification.** Organization shall notify SLP Toolkit promptly of any known or suspected unauthorized access. Organization will assist SLP Toolkit in any efforts by SLP Toolkit to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF SLP TOOLKIT

1. **Privacy Compliance.** The Parties expect that SLP Toolkit may receive personally identifiable information (“PII”) in Student Data from the Organization. SLP Toolkit shall comply with all applicable state and Federal laws and regulations pertaining to data privacy and security, including FERPA and all other applicable privacy statutes. The Parties agree that SLP Toolkit is a “school official” under FERPA and has a legitimate educational interest in PII from Student Data. For purposes of the DSPA, SLP Toolkit:
 - a. provides a service or function for which the Organization would otherwise use employees;

- b. is under the direct control of the Organization with respect to the use and maintenance of education records; and
 - c. is subject to the requirements of FERPA governing the use and redisclosure of Student Data.
- 2. **Employee Obligation.** SLP Toolkit shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DSPA with respect to the data shared under the DSPA. SLP Toolkit agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DSPA.
- 3. **Aggregate Data.** SLP Toolkit may use aggregate data only for the purposes of development, research, and improvement of educational sites, services, or applications. SLP Toolkit agrees not to attempt to re-identify de-identified Student Data. SLP Toolkit shall not copy, reproduce or transmit any Student Data obtained under the DSPA and/or any portion thereof, except as necessary to fulfill the DSPA.
- 4. **Disposition of Student Data.** The Organization has the ability to delete SLP and Student Data associated with their accounts at any time using the software or by special request, except in instances where such data is otherwise prohibited from deletion or required to be retained under state or federal law, or stored as a copy as part of a disaster recovery storage system and that is:
 - a. inaccessible to the public, and
 - b. unable to be used in the normal course of business by SLP Toolkit.

Disposition shall include:

- a. Electronic Student Data record destruction; or
- b. Otherwise modifying Student Data in those records to make it unreadable.

If a special request is made to delete Student Data owned by the Organization, SLP Toolkit shall provide written notification to Organization when the Student Data has been disposed of. The duty to dispose of Student Data shall not extend to data that has been aggregated and de-identified pursuant to the other terms of the DSPA.

The Organization understands and agrees that Student Data backups and audit logs are not easily parsed or accessible, and are not immediately destroyed upon request or the termination of any agreement between the parties.

- 5. **Advertising Prohibition.** SLP Toolkit is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by SLP Toolkit; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other

than providing the Service to the Organization; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Services to the Organization. This section does not prohibit SLP Toolkit from generating legitimate personalized learning recommendations.

6. **Access to Student Data.** If Student Data owned by the Organization is not accessible to the Organization's users by circumstances out of the normal course of operation, SLP Toolkit shall assist to make Student Data available to the Organization within five (5) business days of a request by the Organization.

ARTICLE V: DATA PROVISIONS

1. **Student Data Security.** SLP Toolkit 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 SLP Toolkit are set forth in this DSPA, and specific security measures are published and maintained on the SLP Toolkit website (<https://www.slptoolkit.com/security-procedures/>)
2. **Passwords and Employee Access.** SLP Toolkit shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data by using forms of authentication and encryption consistent with industry standards and technology best practices. SLP Toolkit shall only provide access to Student Data to employees or contractors that are performing the Services.
3. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the access or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. SLP Toolkit shall maintain all data obtained or generated pursuant to the DSPA in a secure environment and not copy, reproduce, or transmit data except as necessary to perform the Services or access data specifically requested by the Organization.
4. **Employee Training.** SLP Toolkit shall provide periodic security training to those of its employees who operate or have access to data and to the system. Further, SLP Toolkit shall provide the Organization with contact information of an employee to answer any security questions and address security concerns.
5. **Security Technology.** When data is accessed using a supported web browser, Secure Socket Layer ("SSL") technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication for account access and data encryption for all Student Data. SLP Toolkit shall host data pursuant to

the DSPA in an environment using a firewall that is periodically updated according to industry standards. Furthermore, reasonable technical methods shall be employed to safeguard data in a manner consistent with ISO 27001/27002 and section 13402(H)(2) of Public Law 111-5.

6. **Subprocessors Bound.** SLP Toolkit may enter into written agreements whereby subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. SLP Toolkit shall periodically conduct or review compliance monitoring and assessments of subprocessors to determine their compliance with this Article.
7. **Periodic Risk Assessment.** SLP Toolkit further agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, SLP Toolkit will provide the Organization with executive summaries of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DSPA.
8. **Backups.** SLP Toolkit agrees to maintain backup copies, backed up at least daily, of Student Data in case of SLP Toolkit's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.
9. **Audits.** Upon receipt of a request from the Organization, SLP Toolkit will allow the Organization to audit the security and privacy measures that are in place to ensure protection of the Student Data. SLP Toolkit will cooperate fully with the Organization and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of SLP Toolkit and/or delivery of Services to the Organization, and shall provide full access to SLP Toolkit's facilities, staff, agents and Organization's Student Data and all records pertaining to SLP Toolkit, Organization and delivery of Services to SLP Toolkit. Failure to cooperate shall be deemed a material breach of the DSPA.

All time spent by SLP Toolkit at the request of the Organization with respect to audits is billable. SLP Toolkit will be compensated by the Organization at the rate of \$100 per hour for audit services rendered. SLP Toolkit will provide a breakdown of hours spent along with an invoice.
10. **Confidentiality Measures.** SLP Toolkit agrees to implement appropriate measures designed to ensure the confidentiality of Student Data and other data, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to the Organization or an individual identified with the data or information in SLP Toolkit's custody.

SLP Toolkit certifies that it has implemented policies and procedures to protect against reasonably foreseeable unauthorized access to, or disclosure of, Student Data or other data, and to prevent other reasonably foreseeable events that may result in substantial harm to the Organization or any individual student.

SLP Toolkit shall not permit Organization data or Student Data to be maintained or stored on any of SLP Toolkit's Mobile Device or Portable Storage Medium unless it is encrypted.

11. **Data Breach.** SLP Toolkit will notify the Organization when there has been an unauthorized release, breach, disclosure, or acquisition of Student Data owned by the Organization. Such notification will follow the standard procedures below. In the event that Student Data is accessed or obtained by an unauthorized individual, SLP Toolkit will notify Organization of the incident within 72 hours of breach confirmation using the following process:
 - a. The security breach notification will be delivered via electronic mail to the Organization, at the email address on file with SLP Toolkit. Every reasonable attempt will be made to obtain confirmation that the information is received.
 - b. The notification will be titled "Notice of Student Data Breach", and will contain the following information:
 - i. What Happened - how the breach was able to occur, and when the breach occurred
 - ii. What Information Was Involved - the specific information that may have been compromised by the breach
 - iii. What We Are Doing - the current and next steps in SLP Toolkit procedures that are being followed
 - iv. What You Can Do - steps Organization can take to help
 - v. For More Information - contact information and resources for additional information
 - c. SLP Toolkit will assist any local education agency to issue additional notifications as required by law.
 - d. Reimbursement for expenses associated with a security breach where the Provider is at fault will be coordinated through the Provider's cyber liability insurance policy. The insurance policy is intended to cover all costs incurred by the LEA resulting from a security breach, subject to the terms and conditions of the insurance policy. Any expenses directly related to a security breach where the Provider is at fault and which are not covered by the insurance policy will be the responsibility of the Provider.

ARTICLE VI: MISCELLANEOUS

1. **Term.** This DSPA will remain in effect for a maximum of one (1) year from the date SLP Toolkit begins providing the Services to the Organization, but shall expire before that time if SLP Toolkit no longer provides the Services to the Organization, or is terminated by either party in accordance with this DSPA. Either party may also terminate this DSPA immediately upon the other party's breach of this DSPA. SLP Toolkit shall be bound by the confidentiality of Student Data provisions of this DSPA for as long as SLP Toolkit possesses the Organization's Data.
2. **Termination.** In the event that either party seeks to terminate this DSPA, they may do so by mutual written consent.
3. **Effect of Termination Survival.** If the DSPA is terminated, SLP Toolkit shall dispose of the Organization's Data as stated in Article IV, section 4, Disposition of Student Data.
4. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery or email transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives:

The designated representative for SLP Toolkit for this DSPA is:

Paul Keck
SLP Toolkit
Privacy Officer
privacy@slptoolkit.com

The designated representative for the Organization for this DSPA is:

Edward Hausauer
Pioneer Central School
Data Protection Officer
ehausauer@piuoneerschools.org

5. **Severability.** Any provision of this DSPA 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 DSPA, 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 DSPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Authority.** SLP Toolkit represents that it is authorized to bind to the terms of this DSPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof is stored, maintained or used in any way.
7. **Waiver.** Waiver by any party to this DSPA of any breach of any provision of this DSPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DSPA shall not operate as a waiver of such right. All rights and remedies provided for in this DSPA are cumulative. Nothing in this DSPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the Organization, its officers, employees, and agents as a result of the execution of this DSPA or performance of the functions or obligations described herein.
8. **Assignment.** None of the parties to this DSPA may assign their rights, duties, or obligations under this DSPA, either in whole or in part, without the prior written consent of the other party to this DSPA.
9. **Amendments To Standard Agreements.** The SLP Toolkit Privacy, Terms of Use, and Standard Terms and Conditions are amended as follows where appropriate:
 - a. If the Organization is a school district or other government entity, all references to indemnification are deleted in their entirety. In this case, the Organization has no express contractual obligation to indemnify or hold SLP Toolkit harmless.
 - b. All references to venue or governing law are modified such that New York law shall govern any disputes, mandatory mediation shall take place in New York, and claims or causes of action arising out of the DSPA must be commenced within three (3) years after the cause of action accrues.
 - c. All references to prevailing party attorney fees are deleted. Each party shall bear its own attorney and legal costs.
 - d. All references to complete agreements are deleted, and this DSPA is included as part of the agreement between the Organization and SLP Toolkit. This DSPA supersedes all other agreements where conflicts arise.

- e. This DSPA supersedes all standard terms and conditions that may be attached to SLP Toolkit generated invoices during the term of this DSPA.

IN WITNESS WHEREOF, the parties have executed this DSPA as of the last day noted below.

SLP TOOLKIT, LLC

Signature:



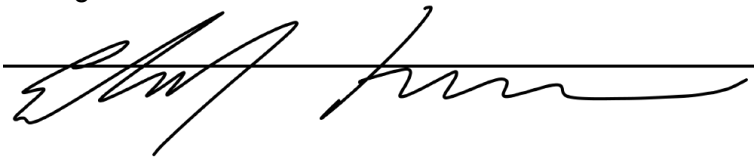
Date: 04-04-2024

Printed Name: Paul Keck

Title/Position: Privacy Officer

Organization:

Signature:



Date: 04-04-2024

Printed Name: Edward Hausauer

Organization Name: Pioneer Central School

Title/Position: Data Protection Officer

CHANGE LOG

Jun 26, 2023

- Added this change log

Jan 23, 2023

- Article 6, Section 1 - Reduced term of the agreement to one year

Oct 7, 2022

- Article I, Section 2 - Expanded description of services to include emails sent to users

Jun 2, 2021

- Article V, Section 11 - Breach notification was reduced to 72 hrs from 30 days
- Article V, Section 11 - Added "section d" about cost reimbursement for breach notifications

May 27, 2021

- Original version, tracking started