



# STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0)

**Provo City School District**

**and**

**LUCID SOFTWARE INC.**

Version: 1r7

© 2021 Access 4 Learning (A4L) Community. All Rights Reserved.

*This document may only be used by A4L Community members and may not be altered in any substantive manner.*

## STANDARD STUDENT DATA PRIVACY AGREEMENT NDPA Standard Version 1.0

Version1r7

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

Provo City School District (School District Name),  
located at 280 W 940 N, Provo, UT 84604 (Street, City,  
State) (the “**Local Education Agency**” or “**LEA**”) and

Lucid Software Inc., located at 10355 South Jordan Gateway, Suite 150, South Jordan, UT 84095 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

**2. Special Provisions. Check if Required**

- If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.

If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit “H”. (Optional)**

If checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three (3) years. **Exhibit “E”** will expire three (3) years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).

6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name: Clint Smith Title: Data Privacy Coordinator

Address: 280 W 940 N, Provo, UT 84604

Email: clints@provo.edu Phone: 801-374-4859

The designated representative for the Provider for this DPA is:

Name: Elliot Smith Title: Sr. Vice President, Finance

Address: 10355 South Jordan Gateway, Suite 150, South Jordan, UT 84095

Phone: 844-465-8243

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**LEA**

By: Clint Smith Date: 9/2/2022

Printed Name: Clint Smith Title/Position: Data Privacy Coordinator

**Lucid Software Inc.**

By: Elliot Smith Date: 9/13/2022

Printed Name: Elliot Smith Title/Position: Sr. Vice President, Finance

## STANDARD CLAUSES

Version 1.0

### ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- 2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
- 3. DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

### ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1. Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA 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 Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- 2. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

- 3. Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said

Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
  3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit “A”** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. Deidentified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data**" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new

education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

## ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or 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 LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- (2) Provider agrees to adhere to all federal and state requirements 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.
- (3) 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 summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service

© Access 4 Learning (A4L) Community Version 1r7 Page 8 of 21  
STANDARD STUDENT DATA PRIVACY AGREEMENT NDPA Standard Version 1.0

Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit "H"**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be

amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.
8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, 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.

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

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

The Subscription Service, Support, Professional Services, and any other services provided by Provider to the LEA as set forth in an applicable Service Agreement or Order, but excludes any application not developed or supported by Provider.

**EXHIBIT "B"****SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics  Assessment    Attendance	Meta data on user interaction with application	X
	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X

Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	

© Access 4 Learning (A4L) Community Version 1r7 Page 12 of 21  
 STANDARD STUDENT DATA PRIVACY AGREEMENT NDPA Standard Version 1.0

Gender	
Ethnicity or race	
Language information (native, or primary language spoken by student)	X

<b>Category of Data</b>	<b>Elements</b>	<b>Check if Used by Your System</b>
	Other demographic information-Please specify:	Full name of users, email address and password
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	

	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	

© Access 4 Learning (A4L) Community Version 1r7 Page 13 of 21  
 STANDARD STUDENT DATA PRIVACY AGREEMENT NDPA Standard Version 1.0

	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	

	Medical alerts/ health data	
--	-----------------------------	--

© Access 4 Learning (A4L) Community Version 1r7 Page 14 of 21  
STANDARD STUDENT DATA PRIVACY AGREEMENT NDPA Standard Version 1.0

## EXHIBIT “C”

### DEFINITIONS

**De-Identified Data and De-Identification:** Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

**Educational Records:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**Operator:** means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

**Student Generated Content:** The term “Student-Generated Content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

**School Official:** For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, 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 service, and who has access to Student Data.

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

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

Provo City School District (Name of District or LEA)

Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By \_\_\_\_\_ (Date)

4. Signature

Elliot Smith

9/13/2022

Authorized Representative of Disposition of Data

LEA 5. Verification of

Date

Clint Smith

9/13/2022

Authorized Representative of Provider Date

**EXHIBIT "E"**

**GENERAL OFFER OF PRIVACY TERMS**

**1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and Provo City School District [Insert Name of Originating LEA] ("Originating LEA") which is dated 9/2/2022 [Insert Date], to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: [Contracts@Lucidchart.com](mailto:Contracts@Lucidchart.com)

**Lucid Software Inc.**

BY: Date: Elliot Smith<sup>9/13/2022</sup>

Printed Name: Elliot Smith Title/Position: Sr. Vice President, Finance

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the Originating LEA and the Provider. **\*\*PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. \*\***

**Subscribing LEA**

BY: Date: Clint Smith<sup>9/13/2022</sup>

Printed Name: Title/Position: Clint Smith SCHOOL DISTRICT NAME: Provo City SD  
Data Privacy Coordinator

Address: \_\_\_\_\_ Telephone number

\_\_\_\_\_ Email \_\_\_\_\_

**EXHIBIT “F”****DATA SECURITY REQUIREMENTS****Adequate Cybersecurity Frameworks**

**2/24/2020** The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* (“Cybersecurity Frameworks”) that may be utilized by Provider.

## Cybersecurity Frameworks

<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

## EXHIBIT “G”

### Supplemental SDPC State Terms for [Utah]

[The State Supplement is an **optional** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (Exhibit “H” in this proposed structure).]

**EXHIBIT “H”**

**Additional Terms or Modifications**

LEA and Provider agree to the following additional terms and modifications:

1. Provider’s Terms of Service (“Service Agreement”), found online at [www.lucid.co/tos](http://www.lucid.co/tos), are hereby incorporated and made part of this Agreement. In the event of a conflict between the terms of the DPA and the Service Agreement, the terms of this DPA shall control with respect to the treatment of Student Data in order to comply with the privacy protections or to the extent required by applicable law, otherwise, the Service Agreement will control.
  
2. Notwithstanding anything to the contrary, this DPA shall stay in effect until the LEA permanently deletes all subscriptions to the Services or the parties enter into a new agreement to supersede this DPA.
  
3. Notwithstanding anything to the contrary, Provider shall delete Student Data solely upon request by LEA.
  
4. Audits may only be conducted following eight- (8-) weeks’ advanced written notice.
  
5. Provider aligns with the CIS Top 20 and NIST Cybersecurity Framework Version 1.1 standards. Additional information regarding Provider’s Software Security Program can be found online at <https://lucid.co/node/396>.
  
6. LEA may only terminate this DPA as a result of a merger, acquisition, consolidation, or other business organization in the event the successor indicates its decision to not honor the obligations of Provider.
  
7. Educational Records are not permitted to be stored or processed in the Services.



**Certificate Of Completion**

Envelope Id: 095797EDC5EB4758A54D589A20216156	Status: Completed
Subject: Please DocuSign: Lucid DPA	
Source Envelope:	
Document Pages: 21	Signatures: 5
Certificate Pages: 5	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Julia Potter
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	jpotter@lucidchart.com
	IP Address: 67.182.234.216

**Record Tracking**

Status: Original 9/12/2022 9:30:45 AM	Holder: Julia Potter jpotter@lucidchart.com	Location: DocuSign
--	--	--------------------

**Signer Events**

Signer Events	Signature	Timestamp
Clint Smith clints@provo.edu Data Privacy Coordinator Provo City SD Security Level: Email, Account Authentication (None)	<i>Clint Smith</i>  Signature Adoption: Pre-selected Style Using IP Address: 158.91.136.3	Sent: 9/12/2022 4:08:34 PM Viewed: 9/13/2022 7:37:34 AM Signed: 9/13/2022 7:43:07 AM

**Electronic Record and Signature Disclosure:**  
Accepted: 9/13/2022 7:37:34 AM  
ID: 8fe129dc-ef11-404a-85a2-f74327025cb7

Elliot Smith esmith@lucid.co SVP Finance Security Level: Email, Account Authentication (None)	<i>Elliot Smith</i>  Signature Adoption: Pre-selected Style Using IP Address: 66.60.102.226	Sent: 9/12/2022 4:08:33 PM Viewed: 9/13/2022 5:45:41 PM Signed: 9/13/2022 5:45:49 PM
--	--	--

**Electronic Record and Signature Disclosure:**  
Accepted: 7/27/2022 9:26:33 AM  
ID: 7d4399c0-ac0a-484a-8520-83d65fb62dcb

**In Person Signer Events**      **Signature**      **Timestamp**

**Editor Delivery Events**      **Status**      **Timestamp**

**Agent Delivery Events**      **Status**      **Timestamp**

**Intermediary Delivery Events**      **Status**      **Timestamp**

**Certified Delivery Events**      **Status**      **Timestamp**

**Carbon Copy Events**      **Status**      **Timestamp**

Sultan Seraj sseraj@lucid.co Security Level: Email, Account Authentication (None)	COPIED	Sent: 9/12/2022 4:08:34 PM Viewed: 9/14/2022 7:49:40 AM
---	--------	--

**Electronic Record and Signature Disclosure:**  
Not Offered via DocuSign

Carbon Copy Events	Status	Timestamp
<p>Cara Frisbie cara@lucid.co General Counsel Cara Frisbie Security Level: Email, Account Authentication (None)</p> <p><b>Electronic Record and Signature Disclosure:</b> Accepted: 9/8/2022 2:36:31 PM ID: 87799896-2b40-4879-b3a0-6fc452579354</p>	<b>COPIED</b>	Sent: 9/13/2022 5:45:51 PM
<p>Clint Smith clints@provo.edu Data Privacy Coordinator Provo City SD Security Level: Email, Account Authentication (None)</p> <p><b>Electronic Record and Signature Disclosure:</b> Accepted: 9/13/2022 7:37:34 AM ID: 8fe129dc-ef11-404a-85a2-f74327025cb7</p>	<b>COPIED</b>	Sent: 9/13/2022 5:45:51 PM
<p>David Palmer dpalmer@lucidchart.com Security Level: Email, Account Authentication (None)</p> <p><b>Electronic Record and Signature Disclosure:</b> Accepted: 8/16/2022 9:27:03 AM ID: d0a5e43d-5625-4342-9bf1-b075c2c23fcd</p>	<b>COPIED</b>	Sent: 9/13/2022 5:45:51 PM
<p>Melinda Hicken mhicken@lucidchart.com Senior Corporate Paralegal Security Level: Email, Account Authentication (None)</p> <p><b>Electronic Record and Signature Disclosure:</b> Accepted: 7/25/2022 1:17:15 PM ID: 2e056ce6-5704-4f46-ab0b-8c83a0a51440</p>	<b>COPIED</b>	Sent: 9/13/2022 5:45:51 PM
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	9/12/2022 4:08:34 PM
Certified Delivered	Security Checked	9/13/2022 5:45:41 PM
Signing Complete	Security Checked	9/13/2022 5:45:49 PM
Completed	Security Checked	9/13/2022 5:45:51 PM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

## **ELECTRONIC RECORD AND SIGNATURE DISCLOSURE**

From time to time, People Ops (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

### **Getting paper copies**

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

### **Withdrawing your consent**

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

### **Consequences of changing your mind**

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

### **All notices and disclosures will be sent to you electronically**

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

### **How to contact People Ops:**

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: [mjarman@lucidchart.com](mailto:mjarman@lucidchart.com)

### **To advise People Ops of your new email address**

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at [mjarman@lucidchart.com](mailto:mjarman@lucidchart.com) and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

### **To request paper copies from People Ops**

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to [mjarman@lucidchart.com](mailto:mjarman@lucidchart.com) and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

### **To withdraw your consent with People Ops**

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to [mjarman@lucidchart.com](mailto:mjarman@lucidchart.com) and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

### **Required hardware and software**

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

### **Acknowledging your access and consent to receive and sign documents electronically**

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to ‘I agree to use electronic records and signatures’ before clicking ‘CONTINUE’ within the DocuSign system.

By selecting the check-box next to ‘I agree to use electronic records and signatures’, you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify People Ops as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by People Ops during the course of your relationship with People Ops.