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

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:

[School District (LEA).Company]   , located at

(the "**Local Education Agency**" or "**LEA**") and

                    , located at

(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~~ and 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, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

    ☒ If checked, LEA and Provider agree to the additional terms of modifications set forth in **Exhibit "H"**.

3. In the event of a conflict between the ~~SDPC~~ Standard Clauses, the Supplemental State Terms or Special Provisions, the Special Provisions will control. In the event there is conflict between the terms of the DPA and any other ~~writing~~ agreement between the Provider and LEA, including, but not limited to ~~the~~any Service Agreement and Provider ~~T~~terms of ~~S~~service or ~~P~~privacy ~~P~~policy the terms of this DPA shall control with respect to the subject matter in conflict.

4. This DPA shall stay in effect for three years. Exhibit E will expire 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.

ARTICLE I: PURPOSE AND SCOPE

3. **DPA Definitions**. The definitions of terms used in this DPA ~~is~~are found in **Exhibit "C"**. ~~In the event of a conflict,~~ When interpreting this DPA, 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 III: DUTIES OF LEA

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or believed unauthorized access to, use of, or acquisition of the Services or the Student Data. If requested by Provider, LEA will provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to any unauthorized access to, use of, or acquisition of the Services or the Student Data.

ARTICLE IV: DUTIES OF PROVIDER

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than providing the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under ~~the statutes referred to herein this DPA~~ applicable laws.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and ~~a~~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 and ~~a~~Agents 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 non-public 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. De-Identified 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

2

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.~~ In accordance with the data retention policy described in Exhibit A*. 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"**.

Note* Exhibit A language will include the following:
Provider needs to provide the detailed retention policy details, including the timeline.

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. Targeted advertising is strictly prohibited. Nothing in this DPA prohibits Provider from Processing Student Data for lawfully permissible purposes ~~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

2. **Audits**. No more than once a year, or following unauthorized access to Student Data in connection with the Services, ~~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.~~ ~~T~~the LEA may make reasonable inquiries of the Provider regarding the use of the LEA's Student Data and the security measures undertaken by the Provider to protect said Student Data. 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 relevant records collectively pertaining to all of the following: 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 consistent with industry standards and 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~~ an industry standard Cybersecurity Framework that may be based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework ~~must~~ may be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its

3

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 ("Data Breach"), the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the ~~incident~~ Data Breach, 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~~ Data Breach. Provider shall follow the following process in connection with a ~~incident~~ Data Breach:

   (1) The ~~security~~ Data ~~b~~Breach ~~incident~~ 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~~ Student Data that were or are reasonably believed to have been the subject of a Data ~~b~~Breach.
      iii. If the information is possible to determine at the time the notice is provided, then either the date of the Data ~~b~~Breach, (2) the estimated date of the Data ~~b~~Breach, or (3) the date range within which the Data ~~b~~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 ~~security~~ Data ~~b~~Breach ~~incident~~, if that information is possible to determine at the time the notice is provided.

   (2) Provider agrees to adhere to all applicable 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 ~~b~~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 applicable 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 written request, with a summary of said written incident response plan~~,~~. In the event said written incident response plan contains sensitive or proprietary information, Provider's provision of such written incident response plan shall be subject to LEA's execution of Provider's non-disclosure agreement.

   (4) LEA shall provide notice and facts surrounding the Data ~~b~~Breach to the affected students, parents or guardians.

   (5) In the event of a Data ~~b~~Breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

4

ARTICLE VII: MISCELLANEOUS

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to support comply compliance with the applicable privacy protections laws, including those found in applicable provisions of 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 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. The total and aggregate liability and indemnity obligations of either Party under this DPA is and shall remain subject to the exclusions, limitations of liability and indemnity provisions set out in the applicable Service Agreement.

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 sSuccessor 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.

EXHIBIT "B"
SCHEDULE OF STUDENT DATA

> Exhibit "B"; pg. 1>
> Exhibit "B"; pg. 2 >
>Exhibit "B"; pg. 3

☐ I have reviewed and selected only the Student Data Elements that we may need to collect in order to

provide the services. This does not, however, preclude LEA from providing additional Student Data.

5

EXHIBIT "C"

DEFINITIONS

Agent is an individual who is not an employee or Subprocessor of the Provider, but who is legally authorized by Provider to act on Provider's behalf in the performance of the Service Agreement.

De-Identified Data ~~and De-Identification~~: ~~Records and information are considered to be de-identified when~~ Data from which 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.

Education~~al~~ Records: Education~~al~~ Records shall have the meaning as defined in FERPA. Education 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, which may include but are not limited to, records in all media 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 constitute De-Identified Data or otherwise have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information or Student Data.

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 educational agency or institution would otherwise use employees; (2) Is under the direct control of the educational 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 Provider's Contract, Purchase Order, ~~or~~ Terms of Service, ~~or~~ Terms of Use, and any other applicable Provider documents incorporated into the agreement between Provider and LEA.

Student Data: Student Data includes any data provided or made available to Provider in connection with the Service Agreement, whether gathered by Provider or provided to Provider by LEA or its users, students, or students' parents/guardians, that ~~is descriptive of the~~ identifies, describes, or reasonably relates to an LEA student including, but not limited to, information in the student's ~~e~~Education~~al~~ ~~r~~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 identifiable information about a specific student. Student Data includes personally identifiable Meta~~ D~~data. Student Data further includes "personally

6

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 applicable federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to may be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute include that information that has been anonymized or dDe-identified Data, 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 in connection with the Service Agreement, and who has access to Student Data.

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 oOperator'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.

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms Provider offers the same privacy protections found in this DPA between it and
[School District (LEA).Company]
("Originating LEA") which is dated*[Document.CreatedDate]* 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, Service Agreement, 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 statutes; (2) a material change in the services and/or 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:

7

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

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	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 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~~

This Amendment for SDPC State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

, located at

(the "**Local Education Agency**" or "**LEA**") and   , located at

(the "**Provide**r").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of ~~p~~Pupil ~~r~~Records; and/or (b) digital educational software that authorizes Provider to access, store, and use ~~p~~Pupil ~~r~~Records; and

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 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties ~~in order~~ and to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in ~~order to~~ compl~~y~~iance with applicable California state laws and regulations.

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

1.   **Term**. The term of this Amendment shall expire on the same date as the DPA, <u>unless otherwise terminated by the Parties.</u>

2.   **Modification to Article IV, Section 7 of the DPA**. Article IV, Section 7 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows: 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. <u>Targeted Advertising is strictly prohibited.</u>

<u>Nothing in this DPA prohibits Provider from processing Student Data for lawfully permissible purposes.</u>~~However, 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 ~~that are not considered Targeted Advertising~~; or (iii) to notify account holders about new education product updates, features, or services ~~that are not considered Targeted Advertising or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits~~.

10

GENERAL OFFER OF PRIVACY TERMS

1. **Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and

Val Verde Unified School District

("Originating LEA") which is dated   Dec 14, 2022   , 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:

_____reema@merlyn.org_____ .

PROVIDER:_____Merlyn Mind, Inc._____

BY: _____*Charles Prestia*_____Date: 12-27-2022_____

Printed Name: _____Charles Prestia_____Title/Position: Senior Vice President and Head of Sales

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   Val Verde Unified School District

and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

LEA:_____

BY:

_____Date:_____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

1190353v1