Applied Survey Research School Readiness Data Entry Platform Privacy Policy

Version: 2.0
Effective 1/22/24

STANDARD CLAUSES

Version 2.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of Privacy Policy**. The purpose of this Privacy Policy 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.

2. **Student Data to Be Provided**. The services to be provided by ASR pursuant to this Policy are detailed in **Exhibit "A."** Database Users will provide Student Data to ASR as identified in the Schedule of Data, attached hereto as **Exhibit "B"**. Categories of data to be supplied to ASR may be modified if said modification is in writing and signed by ASR's and the user's designated representatives. Upon Database User's written request, ASR will provide the user with a data inventory that inventories all data fields and delineates which fields are encrypted within ASR's platform maintaining collected Student Data.

3. **Privacy Policy Definitions**. The definition of terms used in this Privacy Policy is found in **Exhibit "C."** In the event of a conflict, definitions used in this Privacy Policy shall prevail over terms used in any other writing, including, but not limited to the Privacy Policy or Privacy Policies.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of Database User.** All existing Student Data transmitted to ASR identified in **Exhibit "B"**, is and will continue to be the property of and under the control of the Database User. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data shall remain the exclusive property of the Database User. ASR further acknowledges and agrees that all copies of such Student Data transmitted to ASR, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Privacy Policy in the same manner as the original Student Data. ASR further agrees that Student Data cannot be used by ASR for marketing, advertising, or data mining, or shared with any third parties unless allowed by law and expressly authorized by the Database User in writing.

2. **Parent Access**. ASR shall respond in a reasonably timely manner (and no later than thirty (30) days from the date of the request or pursuant to the time frame required under state law for a Database User to respond to a parent or student, whichever is sooner) to the Database User's request for Student Data in a student's records held by ASR to view or correct as necessary. In the event that a parent of a student or other individual contacts ASR to review any of the Student Data accessed pursuant to the Services, ASR shall refer the parent or individual to the Database User, who will follow the necessary and proper procedures regarding the requested information.

3. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact ASR with a request for Student Data held by ASR pursuant to the Privacy Policy, ASR shall notify the Database User in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Database User of the request. ASR will consult with the Database User regarding its response to the request and cooperate with the User's reasonable requests in connection with efforts to intervene and quash or modify the legal order, demand or request; and upon request, provide the Database User with a copy of its response. If the Database User receives a subpoena, warrant, or other legal order, demand or request seeking Student Data maintained by ASR, the Database User will promptly provide a copy of the request to ASR. ASR will promptly supply the Database User with copies of records or

information required for the Database User to respond, and will cooperate with the Database User's reasonable requests in connection with its response.

4. **Subprocessors and Authorized Access**. ASR will provide access to Student Data, including anonymized, only to its employees and subcontractors who need to access the data to fulfill ASR's obligations under this Policy. ASR will ensure that employees and subcontractors who perform work under this Policy have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement. ASR shall enter into written agreements with all subprocessors performing functions for ASR in order for activities pursuant to the Privacy Policy, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this Privacy Policy. Upon request of the Database User, ASR will provide a list of the subprocessors and purpose.

ARTICLE III: DUTIES OF DATABASE USER

1. **Provide Data in Compliance with Applicable Laws**. The Database User shall enter Student Data 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 Database User has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), the Database User shall include a specification of criteria for determining who constitutes a Researcher and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. Database User 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**. The Database User shall notify ASR promptly of any known unauthorized access. Database User will assist ASR in any efforts by ASR to investigate and respond to any unauthorized access.
5. **FERPA Adherence.** The Database User shall only enter into agreements with those organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction, if applicable requirements are met. (§ 99.31(a)(6)). The Database User must record the disclosure made under the studies exception per FERPA 99.32.

ARTICLE IV: DUTIES OF ASR

1. **Privacy Compliance**. ASR shall comply, in all material respects, 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. ASR shall conduct any study using the data in a manner that does not permit personal identification of parents and/or students by anyone other than ASR with legitimate interests. In performing the services outlined in **Exhibit "A"**, ASR shall be considered a School Official with legitimate educational interest, and performing services otherwise provided by the Database User. In this capacity, ASR is subject to the requirements of 34 C.F.R. § 99.33(a) governing the use and redisclosure of PII from education records. ASR agrees to abide by the FERPA limitations and requirements imposed on school officials. ASR will use the Education records only for the purpose of fulfilling its duties under this Policy for Database User's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Policy, required by law, or authorized in writing by the District. ASR shall be under the

direct control and supervision of the Database User, with respect to its use of Student Data. ASR warrants that the service it will provide is fully compliant with and will enable the Database User to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the Database User and/or ASR, including but not limited to: the Children's Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Protection of Pupil Rights Amendment (PPRA); Americans with Disabilities Act (ADA), and Federal Export Administration Regulations.

2. **Authorized Use**. The Student Data shared pursuant to the Privacy Policy, including persistent unique identifiers, shall not be used for any purpose not authorized under the statutes referred to herein this Privacy Policy or other applicable laws.

3. **ASR Employee Obligation**. ASR shall require all of ASR's employees and subprocessors who have access to Student Data to comply with all applicable provisions of this Privacy Policy with respect to the Student Data shared under the Privacy Policy. ASR agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Privacy Policy. ASR agrees that all of its employees, contractors, or agents who have such access to Student Data will be properly vetted to ensure that such individuals have no significant criminal history and that they possess all needed qualifications to comply with the terms of this Policy including but not limited to all terms relating to data and intellectual property protection.

4. **No Disclosure**. ASR 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 Database User or this Privacy Policy. Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of ASR pursuant to this Privacy Policy.

    - ASR will not re-disclose any PII to which ASR has access for the purpose of this study and will only use the PII only to meet the purposes stated and will amend this Privacy Policy should the purpose of use within the study change.
    - ASR will take any necessary steps to maintain the confidentiality of the PII at all stages of the study and will not permit the personal identification of parents and students by anyone other than the representations of ASR with legitimate interests.
    - ASR will conduct any studies so as not to identify students or their parents and will allow internal access to PII from education records only to individuals with a need to know.

5. **De-Identified Data.** ASR agrees not to attempt to re-identify de-identified Student Data. De-identified Data may be used by ASR for those purposes allowed under FERPA and the following purposes: assisting the Database User or governmental agencies in conducting research and other studies; research and development of educational sites, services, or applications; and for adaptive learning purposes and customize student learning. Except for subprocessors, ASR agrees not to transfer de-identified Student Data to any party unless that party agrees in writing not to attempt re-identification and prior written notice has been given to the Database User who has provided prior written consent for such transfer. Prior to publishing any document that names the Database User explicitly or indirectly, ASR shall obtain the Database User's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the Database User, ASR shall dispose of or provide a mechanism for the Database User to transfer Student Data obtained under the Privacy Policy, within sixty (60) days of the date of said request and according to a schedule and procedure as the

Parties may reasonably agree. If no written request from the Database User is received, ASR shall dispose of all Student Data at the earliest of (a) ASR's standard destruction schedule, if applicable; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified. The Database User may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D."** If the Database User and Researcher 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. **Data Transfer Upon Termination or Expiration.** Upon termination or expiration of this Policy, ASR will ensure that all Database User Data are securely returned or destroyed as directed by the Database User. Transfer to the Database User or a third party designated by the Database User shall occur within a reasonable period of time, and without significant interruption in service. ASR shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the Database User or its transferee, and to the extent technologically feasible, that the Database User will have reasonable access to Student Data during the transition. In the event that the Database User requests destruction of its data, ASR agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which the ASR might have transferred Database User data. ASR agrees to provide documentation of data destruction to the Database User. ASR will notify the Database User as soon as reasonably practicable of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the Database User access to ASR's facilities to remove and destroy Database User-owned assets and data. ASR shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the Database User. ASR will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the Database User. ASR will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the Database User, all such work to be coordinated and performed in advance of the formal, final transition date.

8. **Publication of Findings.** ASR shall provide the Database User with the right to review any data 30 days prior to publication and to verify proper disclosure avoidance techniques have been used. Based on Guidance for Reasonable Methods and Written Agreements Publication or Disclosure of De-Identified Student Data. If ASR seeks to further disclose or publicly release Student Data, ASR will provide a deidentification plan that must be approved by the Database User.

    a. ASR may attach a code to each record that may allow the recipient, if no PII is included, to match information received from the source provided that the method by which the records code is assigned is not revealed and the record code is not based on a student's social security number or other personal information.

9. **Advertising Limitations.** ASR will not use, disclose, or sell Student Data for marketing purposes or to inform, influence, or enable targeted advertising or develop a profile of a student, family member/guardian or group, for any purpose other than providing services to the Database User. This section does not prohibit ASR from using Student Data for adaptive learning or customized student learning or to make product recommendations to Database Users or notify account holders about new education product updates, features, or services.

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 Database User, ASR will provide a list of the locations where Student Data is stored. ASR will take reasonable measures, including audit trails, to protect Student Data against deterioration or degradation of data quality and authenticity.

2. **Audits.** No more than once a year, or following data breach, upon receipt of a written request from the Database User with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, ASR will allow the Database User 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 Database User. ASR will cooperate reasonably with the Database User and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of ASR and/or conducting Research, and shall provide reasonable access to ASR's facilities, staff, agents and Database User's Student Data and all records pertaining to ASR, the Database User and conducting research to the Database User. Failure to reasonably cooperate shall be deemed a material breach of the Privacy Policy.

   If ASR must under this Policy create, obtain, transmit, use, maintain, process, or dispose of the subset of Student Data known as Personally Identifiable Information or financial or business data which has been identified to the ASR as having the potential to affect the accuracy of the Database User's financial statements, ASR will at its expense conduct or have conducted at least annually a:

   i. American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objectives deemed sufficient by the District, which attests the Vendor's security policies, procedures and controls;
   ii. vulnerability scan, performed by a scanner approved by the User, of ASR's electronic systems and facilities that are used in any way to deliver electronic services under this Policy; and
   iii. formal penetration test, performed by a process and qualified personnel approved by the User, of ASR's electronic systems and facilities that are used in any way to deliver electronic services under this Policy.

   Additionally, ASR will provide the Database User upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Policy. The Database User may require, at User expense, ASR to perform additional audits and tests, the results of which will be provided promptly to the User.

3. **Data Encryption and Security**. ASR agrees to utilize adequate and appropriate administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use or modification, in accordance with commercial best practices. Such measures will be no less protective than those used to secure ASR's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. ASR shall adhere to any applicable law relating to data security and shall implement an adequate Cybersecurity Framework based on nationally recognized standards set forth in **Exhibit "E".** In conducting data transactions and transfers with the Database User, ASR will ensure that all such transactions and transfers are encrypted. Without limiting the foregoing, ASR warrants that all electronic Student Data will be encrypted in transmission using SSL (Secure Sockets Layer). ASR will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Policy. If included in the scope of the Database User's contract with ASR, ASR will provide to the User a current

certificate of insurance including Cyber Security Insurance coverage for Data Breach.

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 ASR, ASR shall provide notification to Database User 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. ASR will fully investigate the incident and cooperate fully with the Database User's investigation of and response to the incident. ASR 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 ASR and as it becomes available:

      i. The name and contact information of the reporting Database User 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) ASR 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) ASR 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 access or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide Database User, upon request, with a summary of said written incident response plan.

   (4) Database User shall provide notice and facts surrounding the breach to the affected students, parents, or guardians. Except as otherwise required by law, ASR will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the Database User.

   (5) In the event of a breach originating from the Database User's use of the Service, ASR shall cooperate with the Database User to the extent necessary to expeditiously secure Student Data. ASR shall reasonably cooperate in the Database User's investigation and third-party notifications, if any, at the Database User's direction and expense.

ARTICLE VI: MISCELLANEOUS

1. **Priority of Agreements**. This Privacy Policy 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 Privacy Policy. In the event there is conflict between the terms of the Privacy Policy, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this Privacy Policy shall apply and take precedence.

2. **Severability**. Any provision of this Privacy Policy 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 Privacy Policy, 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 Privacy Policy or affecting the validity or enforceability of such provision in any other jurisdiction.

3. **Governing Law; Venue and Jurisdiction**. This Privacy Policy will be governed by and construed in accordance with the laws of the state of the Database User, 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 Database User for any dispute arising out of or relating to this policy or the transactions contemplated hereby.

4. **Successors Bound**: This Privacy Policy is and shall be binding upon the respective successors in interest to ASR 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 ASR sells, merges, or otherwise disposes of its business to a successor during the term of this Privacy Policy, ASR shall provide written notice to the Database User 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 Privacy Policy and any obligations with respect to Student Data within the Privacy Policy.

5. **Authority.** Each party represents that it is authorized to bind to the terms of this Privacy Policy, 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.

6. **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.

If you have any questions about this Privacy Policy, you can contact us by email:
Sra@appliedsurveyresearch.org

EXHIBIT "A"

DESCRIPTION OF SERVICES

ASR provides and maintains a secure online database platform to allow for the collection of School Readiness Assessment data: https://schoolreadinessassessment.org. The system is used by the Database User to enter proficiency ratings for kindergarten and pre-K students from the Kindergarten Observation Form (KOF) and Pre-Kindergarten Observation Form (P-KOF) as well as personal identifiers as outlined in Exhibit "B". The platform also uses scores on the KOF and P-KOF to determine whether the child is ready for kindergarten overall and in various domains of readiness.

Classroom teachers enter and view data and run aggregate reports only for students in their class. Authorized school administrators enter and view data and run aggregate reports for students in their schools. Authorized district administrators enter and view data and run aggregate reports for students in their districts. To provide research and evaluation services, ASR will have access to KOF and P-KOF data for all students participating in the assessment.

For the purposes of account creation, the online database system also stores the Database User's name, email address, and school and district of employment, where applicable.

EXHIBIT "B"

SCHEDULE OF DATA

By checking the boxes below, ASR agrees to abide by the following FERPA Studies exception implementation regulations and Database User requirements:

Category of Data	Elements	Check if Used
Application Technology Metadata	IP Addresses of users, Use of cookies, etc.	
	Other application technology metadata - Please specify:	
Application Use Statistics	Metadata on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data - Please specify: Kindergarten Observation Form Pre-Kindergarten Observation Form	X
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X

Category of Data	Elements	Check if Used
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information - Please specify: Proficiency in English	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information - Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	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	

Category of Data	Elements	Check if Used
Special Indicator	English language learner information	X
	Low-income status	
	Medical alerts/ health data	
	Student disability information	X
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information - Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	

Category of Data	Elements	Check if Used
Student work	Student generated content; writing, pictures, etc.	
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	

EXHIBIT "C"

DEFINITIONS

Breach of Security: a successful attempt by an attacker to gain unauthorized access to an organization's computer systems

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, whether through single or multiple releases, and taking into account other reasonably available information 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 a Database User to provide a service to that Database User shall be considered an "operator" for the purposes of this section.

Persistent Unique Identifiers: A persistent identifier is a unique identifier that can be used to recognize a consumer, a family, or a device across different services.

School Official: For the purposes of this Policy 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 redisclosure of personally identifiable information from Education Records.

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.

Student Data: Student Data includes any existing data, whether gathered by ASR or provided by Database User or its users, students, or students' parents/guardians, that is descriptive of the student. This includes data or other direct or indirect identifiers, that are 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 Metadata. 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 Privacy Policy, and for the purposes of federal, state, and local laws and regulations. Existing Student Data as specified in **Exhibit "A"** is confirmed to be collected or processed by ASR 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 ASR's services.

Subprocessor: For the purposes of this Privacy Policy, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than the Database User or ASR, who ASR uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or Database User**] directs ASR to dispose of data obtained by ASR. 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 [Insert Date]

4. Signature

_____ _____

Designated Representative of Database User Date

5. Verification of Disposition of Data

_____ _____

Designated Representative for ASR Date

Exhibit "E"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks.

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 ASR.

	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://edspex.org for further details about the noted frameworks.

.