Appendix A
Data Sharing Agreement

This Data Sharing Agreement ("DSA") is entered into between Graduation Alliance, Inc ("Provider") and the State of Arkansas Department of Education - DESE ("DESE"). This DSA supplements Service Contract number _____ between Provider and DESE relating to the attendance recovery project. Educational agencies or institutions which opt-in to participation in the attendance recovery project in accordance with the Agreement and this DSA (referred to in the Agreement as "Participating Districts and Charter Schools") are referred to individually in this DSA as a "District" and Provider is bound by this DSA to each Participating District and Charter School individually.

This DSA has the following overriding goals:

1. Preserving the confidentiality of Student identities, including assurance that identifiable Student Data is not released to third parties;

2. Enhancing the ability of Provider and the District to improve academic achievement for Students by allowing access to individual Student Records; and

3. Accurately measuring Provider and the District's progress toward improving Student outcomes and indicators, and meeting set targets and other goals using data shared between the Parties.

NOW, THEREFORE, PROVIDER AND REQUESTOR AGREE AS FOLLOWS:

I. DEFINITIONS

The following definitions apply to this document:

a. "Student" is defined as any individual who is or has been in attendance, whether in-person or online, with District, and regarding whom the District maintains education records.

b. "Personally Identifiable Information" ("PII") is as defined in the Family Educational Rights and Privacy Act ("FERPA"), as set forth at 20 U.S.C. § 1232g, 34 CFR Part 99, and if applicable as defined in related state laws and regulations pertaining to the state in which the Student resides.

c. "Education Records" is as defined in FERPA and if applicable as defined in related state laws and regulations pertaining to the state in which the Student resides.

d. "Student Data" is the combination in any form of Personally Identifiable Information and Education Records.

II. OBLIGATIONS OF PROVIDER

The Provider, representing all members of the organization, shall ensure the confidentiality of Student Data through the following methods:

a. The Provider's data custodian(s) designated in Section II(k) shall have completed commercially-reasonable training in the handling and maintenance of Student Data.

b. The Provider shall strictly comply with all state and federal laws that apply to the use and release of the Student Data. When necessary to comply with these laws, the Provider shall procure the consent of parents or eligible Students, as required under applicable law, to the release and use of the Student Data, and shall

maintain and make written proof of parent or Student (if Student is over the age of 18) consent available to Provider.

c. The Provider shall comply with the re-disclosure limitations set forth in FERPA, including 34 C.F.R. § Part 99.33.

d. The Provider shall restrict access to the data only to (i) the person or persons who provide direct services to Students enrolled under the Master Agreement; or (ii) the person or persons within the Provider's organization who have been tasked with analyzing the data; and make those persons aware of, and agree to abide by, the terms set forth in this DSA.

e. The Provider shall not release or otherwise reveal, directly or indirectly, the Student Data to any individual, agency, entity, or third party not included in this DSA, unless such disclosure is required by law or court order.

f. The Provider shall not distribute, reprint, alter, sell, assign, edit, modify or create derivative works or any ancillary materials from or with the Student Data without the express written consent of Provider, and if necessary, based upon FERPA and its regulations, Students and/or their parents.

g. The Provider shall not use Student Data shared under this DSA for any purpose other than the goals outlined in this DSA. Nothing in the DSA shall be construed to authorize Provider to have access to additional Student Data from Provider that is not included in the scope of the DSA (or addenda). Provider understands that the DSA does not convey ownership of the Student Data to Provider.

h. The Provider shall take commercially-reasonable security precautions and protections to ensure that persons not authorized to view the Student Data do not gain access to the Student Data. Commercially-reasonable security precautions and protections include, but are not limited to:

1. Creating, distributing, and implementing data governance policies and procedures which protect Student Data through appropriate administrative, technical, and physical security safeguards, and outline staff responsibilities for maintaining data security;
2. Encrypting all Student Data carried on mobile computers/devices;
3. Encrypting all Student Data stored in Provider's databases or other storage and access media;
4. Encrypting Student Data before it is transmitted electronically;
5. Requiring that users be uniquely identified and authenticated before accessing Student Data;
6. Establishing and enforcing well-defined data privilege rights which restrict users' access to the Student Data necessary for them to perform their job functions;
7. Ensuring that all staff accessing Student Data sign a commercially-reasonable non-disclosure agreement;
8. Securing access to any physical areas/electronic devices where Student Data are stored;
9. Installing technology necessary to provide commercially-reasonable security for network transmissions involving Student Data;
10. Installing commercially-reasonable anti-virus, network intrusion, logging and notification systems to protect the network and computers where Student Data is stored and accessed;

i. The Provider shall report all known or suspected breaches of Student Data, in any format, to District's data reporting team at _____ within twenty-four (24) hours of confirming or reasonably suspecting such a breach. The report shall include (1) the name, job title, and contact information of the person reporting the incident; (2) the name, job title, and contact information of the person who discovered the incident; (3) date and time the incident was discovered; (4) nature of the incident (e.g., system level electronic breach, an electronic breach of one computer or device, or a breach of hard copies of records; (5) a description of the information lost or compromised; (6) name of electronic system and possible interconnectivity with other systems; (7) storage medium from which information was lost or compromised; (8) controls in place to prevent unauthorized use of the lost or compromised information; (9) number of individuals potentially affected; and (10) whether law enforcement was contacted.

j. The Provider shall securely and permanently destroy the Student Data, and any and all hard and soft (electronic) copies thereof, upon the termination of this DSA or the Master Agreement. Provider agrees to require all employees, contractors, or agents of any kind using Student Data to comply with this provision. Provider agrees to document the methods used to destroy the Student Data, and upon request, provide written certification to Provider that the Student Data has been destroyed.

k. For purposes of this DSA and ensuring Provider's compliance with the terms of this DSA and all applicable state and Federal laws, Provider will designate a custodian of the Student Data that Provider shares with the Provider. Provider will release all Student Data and information under this DSA to said named custodian (the "Data Custodian") in Section VI of this DSA. The Data Custodian shall be responsible for transmitting all Student Data requests and maintaining a log or other record of all Student Data requested and received pursuant to the DSA, including confirmation of the return or destruction of Student Data as described below.

l. Provider or its agents may, upon request, review the records the Provider is required to keep under this DSA. Provider designates its Chief Technology Officer (or an alternative designee specified in writing) as its liaison for all communications with the Provider regarding this DSA;

m. The Provider acknowledges that any violation of this DSA and/or the provisions of FERPA or accompanying state regulations related to the nondisclosure of protected Student information constitutes just cause for Provider to immediately terminate this DSA and the Master Agreement.

III. OBLIGATIONS OF DISTRICT

During the term of this Agreement, District, after opting into this Agreement, shall prepare and deliver to Provider the Student Data as defined in Exhibit A - Data File Description.

IV. PAYMENT

No payments will be made under this DSA by either party.

V. INDEMNIFICATION

a. Provider agrees that to the fullest extent permitted by law, Provider will hold harmless, defend, and indemnify the District, its agents, employees, and board members from any liability, cost or expense, including without limitation penalties, losses, damages, attorneys' fees, taxes, expenses of litigation, judgments, suits, liens, and encumbrances, to the extent arising out of or resulting from any act or omission by Provider under this DSA. The terms of this section shall survive termination of this DSA.

VI. TERM

The Term of this DSA is from the effective date of the above referenced Service Contract until the conclusion of said agreement.

This DSA will allow for the District to provide GA with Student Data, as defined in Exhibit A, for the Term specified above. The DSA shall become effective on the date when the last party to sign has executed this DSA unless terminated under the terms of Paragraph VII below. This DSA may be extended upon mutual written agreement.

VII. TERMINATION

Either party may terminate this DSA, with 30 days written notice to the other party, at any time, for any reason. In addition, District may terminate this DSA with immediate effect if it determines such action is necessary for the health, safety or education of Students or staff.

VII. MISCELLANEOUS PROVISIONS

a. Amendment. Modifications to this DSA must be in writing and be signed by each party.
b. Governing Law. The terms of this DSA shall be interpreted according to and enforced under the laws of the State of Arkansas. The parties agree that any judicial proceedings filed by the parties regarding this DSA will take place in Arkansas.
c. Severability. If any provision of this DSA is held invalid or unenforceable, the remainder of the DSA shall continue in full force and effect.
d. Assignment. Neither party shall assign its rights or responsibilities under this DSA, unless it receives written permission from the other party.
e. Non-Waiver. Any express waiver or failure to exercise promptly any right under this DSA will not create a continuing waiver or any expectation of non-enforcement.
f. Counterparts. The parties agree that this DSA may be executed in one or more counterparts, each of which shall constitute an enforceable original of the DSA, and that facsimile signatures shall be as effective and binding as original signatures.
g. Debarment. District, upon opting into this Agreement, warrants that it is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions (defined as not being eligible to receive federal funds) by any local, state or federal department or agency.
h. Cooperation with Provider Auditor: District, upon opting in to this Agreement, agrees to provide reasonable cooperation with any inquiry by either Provider or 3rd party auditors retained by Provider relating to the performance of this Agreement.