AGREEMENT
(Launch Program – Member District Agreement)

This Agreement ("Agreement") is by and between the Board of Education for the _____ _____ ("Member District") and the Board of Education for the School District of Springfield, R-12 ("SPS'), as the Missouri Fiscal Agent for the Launch Program ("Launch").

1. The Parties.

1.1 SPS – SPS is an urban public school district and a political subdivision of the State of Missouri which is governed by its Board of Education. SPS is the Missouri Fiscal Agent for Launch. SPS's Administrative offices are located at 1359 E. St. Louis Street, Springfield, MO 65802.

1.2 Member District – Member District is a public school district and a political subdivision of the State of Missouri which is governed by its Board of Education. Member District's Administrative offices are located at _____, MO _____. Member District is a member of the Launch Program.

1.3 Independent Contractor -- In the performance of all services covered by this Agreement, SPS and Member District shall be deemed to be and shall be an independent contractor of the other.

1.4 No Agency -- In the performance of all services covered by this Agreement, neither party is authorized or empowered to act as agent for the other for any purpose and shall not on behalf of the other enter into any contract, warranty or representation as to any matter. Neither shall either be bound by the acts or conduct of the other unless specifically set forth in this Agreement or as approved by the respective Boards of the Parties and thereafter authorized in writing by the Parties.

2. The Launch Program.

2.1 Launch is a Statewide program which provides Missouri students access to high quality virtual courses that are designed, developed and delivered by Missouri educators. Students in the Launch Program have access to courses that are not available from their school and/or additional flexibility in scheduling and credit recovery opportunities.

2.2 This Agreement constitutes an intergovernmental agreement pursuant to Section 70.220 RSMo., which allows the Member District to provide the Launch Program to its students.

3. Compliance with Law.

3.1 No Discrimination -- SPS and Member District shall comply with all applicable Federal and State statutes, regulations and guidelines, the Constitutions of the United States and Missouri with respect to the Launch Program. Without limiting the foregoing, SPS and Member District further agree that while engaged in the Launch Program and activities pursuant to this

Agreement, neither of them shall discriminate against any applicant for admission to the Launch Program, participant in the Launch Program, employee or applicant for employment on the basis of the person's race, color, national origin, sex, ancestry, religion, age, physical or mental disability, status as a veteran or any other classification protected by applicable Federal, State or Local law or ordinance.

3.2 Compliance with the Family Educational Rights and Privacy Act – SPS and Member District shall maintain confidentiality concerning personally identifiable information about their respective students who enrolled in the Launch Program as required by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, *et seq.* and its regulations, 34 C.F.R. Part 99 ("FERPA") and Section 167.020.7 RSMo.

4.0 Launch Program Responsibilities.

4.1 Responsibilities of SPS – During the Term of this Agreement, SPS will have the following responsibilities with respect to the Launch Program. SPS will:

(a) Provide the Launch Program curriculum;

(b) Serve as the fiscal agent and administer the Launch Program;

(c) Organize an advisory council made up of member districts and other stakeholders to provide regular feedback regarding Launch Program performance and recommendations regarding future improvements;

(d) Invoice Member District and monitor payments;

(e) Designate a Launch Program Coordinator who will provide support to Member District;

(f) Provide marketing materials to Member District;

(g) Provide Member District access to all Launch Program courses; and,

(h) Perform any other duties deemed necessary for the administration of the Launch Program.

4.2 Responsibilities of Member District – During the Term of the Agreement, Member District will have the following responsibilities with respect to the Launch Program. Member District will:

(a) Provide its students the opportunity to enroll in the Launch Program courses and Member District will pay for these courses;

(b) Designate a Member District Liaison from their school who will work with SPS to enroll students, monitor and receive course grades and act as a single point of

communication. Member District's designated liaison may designate other employees at the Member District to enroll students, monitor, and receive course grades;

(c) Be responsible for paying all costs associated with lost materials provided through the Launch Program including, but not limited to, Chromebooks and heart-rate monitors;

(d) Support the Launch Program by paying membership fees and tuition fees based on enrollment. Current fees are published by SPS and shall be provided upon request. Payments are due thirty (30) days from date of invoice.

(e) Enroll students in the Launch Program using the Launch Program's enrollment platform;

(f) Be responsible for any student counseling or course recommendations related to the Launch Program;

(g) Comply with Section 162.1250, RSMo. including, but not limited to, reporting attendance; and,

(h) Comply with SPS Board of Education Policy EHBC, with regard to data governance and security. Policy EHBC is attached as Exhibit A.

5.0 Student Discipline or Termination from the Launch Program.

5.1 Compliance with SPS Board of Education Policies -- The parties acknowledge that student discipline or termination from the Launch Program must be handled by the Member District in a legally appropriate manner and in accordance with State and Federal law.

6.0 Protection of Launch Program Materials.

6.1 Ownership of Intellectual Property -- SPS and Member District agree that SPS owns all exclusive intellectual property rights, including the copyright, to any curriculum or course materials provided by SPS for the Launch Program. Member District agrees to only use the Launch Program curriculum and course materials in accordance with this Agreement, and not to duplicate, copy, reproduce, sell, distribute or alter any of the Launch Program curriculum or course materials, without express written consent of SPS. Member District further agrees to immediately notify SPS if it becomes aware that the use of the Launch Program curriculum or course materials is not authorized by this Agreement.

6.2 No Transfer of Title or Ownership of Launch Program Curriculum or Course Materials -- Member District understands and agrees that all Launch Program curriculum and course materials have been developed, are owned by SPS. No title or ownership of any portion of the Launch Program curriculum and/or course materials, including but not limited to the proprietary or intellectual property rights related therein, is transferred by this Agreement. SPS

7.0 Term and Termination of Agreement.

7.1 Term of Agreement and Extension -- This Agreement shall be for a period beginning on July 1, 2019 and ending on July 31, 2020, subject to the provisions of this Agreement. This Agreement shall automatically renew for additional Terms of one (1) year, which shall begin on August 1 and end on the following July 31, unless either party provides written notice to terminate the Agreement.

7.2 Termination of Agreement – This Agreement may be terminated as follows:

(a) If either Party gives thirty (30) days written notice to the other Party.

(b) By SPS if the Member District commits a material breach of the Agreement and fails to cure the breach within thirty (30) days following receipt of written notice of its breach from SPS of its breach by SPS.

8.0 <u>Notices and Designated Representatives.</u>

8.1 Notices to SPS -- Any notices required by this Agreement shall be given by hand delivery or by prepaid, first class, certified mail, return receipt requested, addressed in the case of SPS to the persons and at the addresses set forth below, or to their designees or successors at such other addresses as may be given from time to time in accordance with the terms of this notice provision:

<u>SPS Representative</u>:
Ms. Carol Embree
Deputy Superintendent-Operations
School District of Springfield, R-12
1359 E. St. Louis Street
Springfield, Missouri, 65802

8.2 Notices to Member District -- Any notices required by this Agreement shall be given by hand delivery or by prepaid, first class, certified mail, return receipt requested, addressed in the case of Member District to the persons and at the addresses set forth below, or to their designees or successors at such other addresses as may be given from time to time in accordance with the terms of this notice provision:

<u>Member District's Representative</u>:
_____
_____
_____
_____
_____

9.0 Miscellaneous.

9.1 Entire Agreement -- This Agreement constitutes the entire and only agreement between the Parties relating to the Launch Program, and all prior negotiations, representations, agreements and understandings are superseded hereby with relationship to the Launch Program. No agreements altering or supplementing the terms hereof may be made except by means of a written document signed by the duly authorized representatives of the parties.

9.2 Governing Law/Venue -- This Agreement shall be governed, construed and enforced in accordance with the laws of the State of Missouri. Both Parties agree that venue shall be proper in the United States District for the Western District of Missouri, Southern Division, or the Circuit Court of Greene County, Missouri.

9.3 No Assignment -- The rights and obligations provided under this Agreement are not assignable without written consent of the non-assigning party. Any such assignment made or attempted without such required consent is void.

9.4 Authority To Execute Agreement -- The undersigned certify that prior to signing this Agreement, each has received written authorization from his/her respective governing body to sign this Agreement on its behalf.

Organization: The School District of Springfield, R-12

Name: _____ *Date:* _____
School District of Springfield, R-12, Board President

Organization: _____

Name: _____ *Date:* _____
Authorized Signer

Exhibit A
Board of Education Policy EHBC

Policy Descriptor Code: EHBC
DATA GOVERNANCE AND SECURITY

To accomplish the district's mission and comply with the law, the district must collect, create and store information. Accurately maintaining and protecting this data is important for efficient district operations, compliance with laws mandating confidentiality, and maintaining the trust of the district's stakeholders. All persons who have access to district data are required to follow state and federal law, district policies and procedures, and other rules created to protect the information.

Definitions
Confidential Data/Information – Information that the district is prohibited by law, policy or contract from disclosing or that the district may disclose only in limited circumstances. Confidential data includes, but is not limited to, personally identifiable information regarding students and employees.

Critical Data/Information – Information that is determined to be essential to district operations and that must be accurately and securely maintained to avoid disruption to district operations. Critical data is not necessarily confidential.

Responsibility and Data Stewardship
All district employees, volunteers and agents are responsible for accurately collecting, maintaining and securing district data including, but not limited to, information that is confidential or is critical to district operations.

Information Security Officer
The director of information technology is the district's information security officer (ISO) and reports directly to the superintendent or designee. The district's information security officer is directed to create and review district procedures on collecting and protecting district data including, but not limited to, securely maintaining confidential and critical information. The ISO is responsible for implementing and enforcing the district's security policies and procedures applicable to electronic data and suggesting changes to these policies and procedures to better protect the confidentiality and security of district data. The ISO will work with the district's technology department to advocate for resources and implement best practices to secure the district's data.

The manager of infrastructure is the district's alternate ISO and will assume the responsibilities of the ISO when the ISO is not available.

Data Managers
All district administrators are data managers for all data collected, maintained, used and disseminated under their supervision as well as data they have been assigned to manage in the district's data inventory. Data managers will monitor employee access to the information to

ensure that confidential information is accessed only by employees who need the information to provide services to the district and that confidential and critical information is modified only by authorized employees. Data managers will assist the ISO in enforcing district policies and procedures regarding data management.

Confidential and Critical Information

The district will collect, create or store confidential information only when the superintendent or designee determines it is necessary. The district will provide access to confidential information to appropriately trained district employees and volunteers only when the district determines that such access is necessary for the performance of their duties. The district will disclose confidential information only to authorized district contractors or agents who need access to the information to provide services to the district and who agree not to disclose the information to any other party except as allowed by law and authorized by the district.

District employees, contractors and agents will notify the ISO or designee immediately if there is reason to believe confidential information has been disclosed to an unauthorized person or any information has been compromised, whether intentionally or otherwise. The ISO or designee will investigate immediately and take any action necessary to secure the information, issue all required legal notices and prevent future incidents. When necessary, the district's superintendent, ISO or designee is authorized to secure resources to assist the district in promptly and appropriately addressing a security breach.

Likewise, the district will take steps to ensure that critical information is secure and is not inappropriately altered, deleted, destroyed or rendered inaccessible. Access to critical information will only be provided to authorized individuals in a manner that keeps the information secure.

All district staff, volunteers, contractors and agents who are granted access to critical and confidential information are required to keep the information secure and are prohibited from disclosing or assisting in the unauthorized disclosure of confidential information. All individuals using confidential and critical information will strictly observe protections put into place by the district including, but not limited to, maintaining information in locked rooms or drawers, limiting access to electronic files, updating and maintaining the confidentiality of password protections, encrypting and redacting information, and disposing of information in a confidential and secure manner.

Using Online Services and Applications

District staff members are encouraged to research and utilize online services or applications to engage students and further the district's education mission. However, before any online service or application is purchased or used to collect or store confidential or critical information, including confidential information regarding students or employees, the ISO or designee must approve the use of the service or application and verify that it meets the requirements of the law and Board policy and appropriately protects confidential and critical information. This prior approval is also required when the services are obtained without charge.

Training

The ISO will provide appropriate training to employees who have access to confidential or critical information to prevent unauthorized disclosures or breaches in security. In accordance with law, all school employees will receive annual training in the confidentiality of student records.

Data Retention and Deletion
The ISO or designee shall establish a retention schedule for the regular archiving and deletion of data stored on district technology resources. The retention schedule must comply with the Public School District Records Retention Manual as well as the General Records Retention Manual published by the Missouri Secretary of State.

Litigation Hold
In the case of pending or threatened litigation, the district's attorney will issue a litigation hold directive to the superintendent or designee. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by the district's attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by the district's information technology department until the hold is released. No employee who has been notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Consequences
Employees who fail to follow the law or district policies or procedures regarding data governance and security may be disciplined or terminated. Volunteers may be excluded from providing services to the district. The district will end business relationships with any contractor who fails to follow the law, district policies or procedures, or the confidentiality provisions of any contract. In addition, the district reserves the right to seek all other legal remedies, including criminal and civil action and seeking discipline of an employee's teaching certificate.

The district may suspend all access to data or use of district technology resources pending an investigation. Violations may result in temporary, long-term or permanent suspension of user privileges. The district will cooperate with law enforcement in investigating any unlawful actions. The superintendent or designee has the authority to sign any criminal complaint on behalf of the district.

Any attempted violation of district policies, procedures or other rules will result in the same consequences, regardless of the success of the attempt.