VERMONT K-12 STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Addison Central School District

and

ManageBac

November 1, 2018

This Vermont Student Data Privacy Agreement ("DPA") is entered into by and between the Addison Central School District (hereinafter referred to as "LEA") and ManageBac (hereinafter referred to as "Provider") on November 1, 2018. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated November 1, 2018 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; and the Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, this Agreement complies with Vermont laws and Federal Law.

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, and other applicable Vermont State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Managebac is a web-based planning, assessment and reporting platform for the International Baccalaureate program.

3. **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B"

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and all other privacy statutes.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (34 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, and all other privacy statutes.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any

other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and 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 LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

   a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3, above.

   b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

    b. **Destruction of Data**. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

    c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

    d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

    e. **Security Technology**. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

    f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty eight (48) hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.
ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable State and in federal law 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.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

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

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. .

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b), and Article II, section 3, above.

4. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be

in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: _Will Hatch_____
Title: ___Director Of Technology_____
Contact Information: __(802) 382-1284_____
___whatch@acsdvt.org_____

The designated representative for the Provider for this Agreement is:

Name: _Stephen Worden_____
Title: ___Regional Director, Americas_____
Contact Information: __stephen.worden@managebac.com_____
___1.415.483.6365_____

b. Notification of Acceptance of General Offer of Terms. Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: __Stephen Worden_____
Title: ___Regional Director, Americas_____
Contact Information: _stephen.worden@managebac.com_____
__1.415.483.6365_____

6. **Entire Agreement**. This DPA constitutes 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.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. This DPA will be governed by and construed in accordance with the laws of the State of Vermont, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction of Vermont's state and federal courts for any dispute arising out of or relating to this service agreement or the transactions contemplated hereby.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. **Waiver**. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. **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.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Student Data Privacy Agreement as of the last day noted below.

Name of Provider

BY: _____ Date: November 01, 2018

Printed Name: Stephen Worden Title/Position: Regional Director, Americas

Name of Local Education Agency

BY: Will Hatch Date: 11-1-2018

Printed Name: Will Hatch Title/Position: Director of Technology

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

ManageBac is a web-based planning, assessment and reporting platform for the International Baccalaureate program.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	X
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	

Category of Data	Elements	Check if used by your system
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	X
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	

Category of Data	Elements	Check if used by your system
	Low income status	
	Medical alerts /health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading	

Category of Data	Elements	Check if used by your system
	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	
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	

Category of Data	Elements	Check if used by your system
	Other transportation data -Please specify:	

Category of Data	Elements	Check if used by your system
Other	Please list each additional data element used, stored or collected by your application	X

No Student Data Collected at this time _____.
*Provider shall immediately notify LEA if this designation is no longer applicable.

Product Data Field List

The purpose of collecting potentially personally-identifying and personally-identifying information is to provide for the operation of the ManageBac service to allow students, teachers and coordinators to effectively manage their IB programs online. The scope of this varies by user role and the level of implementation, but for students this encompasses class management, upload of coursework, tracking academic progress including grades & attendance.

	Data Collected for Operation	Purpose of Data Collection
1	Student First and Last Name	Required to support product functionality
2	Student Year Level	Required to support product functionality
3	Student Email Address	Required to support product functionality
4	Student Password	Required to support product functionality
5	Student ID Number	Required to support product functionality
6	Student Gender	Required to support product functionality
7	Student DOB	Required to support product functionality
8	Student Languages	Required for IB exam registration
9	Student Nationality	Required for IB exam registration
10	Student IBIS Personal Code	Required for IB exam registration
11	Student Free or Reduced Lunch	Required for IB exam registration
12	Student SSN Last 4 Digits	Required for IB exam registration
13	Student Activities	Required to support product functionality
14	Student Grades	Required to support product functionality
15	Student University List	Required for the IB Student Registry
16	Student Address and Telephone	Required to support product functionality
17	Parent(s) First and Last Name	Required to support product functionality
18	Parent(s) Email Address	Required to support product functionality
19	Parent(s) Password	Required to support product functionality
20	Parent(s) Phone Number	Optional
21	Teacher First and Last Name	Required to support product functionality
22	Teacher Email Address	Required to support product functionality
23	Teacher Password	Required to support product functionality
24	Teacher Phone Number	Optional
25	Admin First and Last Name	Required to support product functionality
26	Admin Role	Required to support product functionality
27	Admin Email Address	Required to support product functionality
28	Admin Password	Required to support product functionality
29	Admin Phone Number	Optional
30	School Name	Required to support product functionality (to identify school network)
31	School Address	Required to support product functionality (to identify school network)
32	Geolocation: coarse (city-level) location data	Required to support product functionality
33	Browser Type	User research to improve ManageBac experience
34	Machine Model	User research to improve ManageBac experience
35	Access Time	User research to improve ManageBac experience
36	Referring URLs	User research to improve ManageBac experience
37	PAGE VIEWS	User research to improve ManageBac experience
38	IP Address	User research to improve ManageBac experience
39	Device ID	User research to improve ManageBac experience
40	Device Type and OS	User research to improve ManageBac experience

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the 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. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Operator: The term "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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in applicable state statues.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the

purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement 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 education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing 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, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Vermont and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Student Personal Information: "Student Personal Information" means information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student that is linked to information that identifies an individual student. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

Sub-processor: For the purposes of this Agreement, the term "Sub-processor" (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 software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated

content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the Service Agreement between LEA and Company. The terms of the Disposition are set forth below:

Extent of Disposition Disposition shall be:	____ Partial. The categories of data to be disposed of are as follows: [INSERT CATEGORIES] _X___ Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	__X__ Destruction or deletion of data. ____ Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	__X__ As soon as commercially practicable _____By (Insert Date) _____ [Insert special instructions.]

Will Patch
Authorized Representative of LEA

11-1-2018
Date

Stephen Worden
Verification of Disposition of Data
by Authorized Representative of Provider

November 01, 2018
Date

OPTIONAL EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer though its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. 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 provide by 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 subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

ManageBac

BY: _____ Date: November 01, 2018

Printed Name: Stephen Worden Title/Position: Regional Director, Americas

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's individual information is contained on the next page. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DATE: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name _____

Title _____

Address _____

Telephone Number _____

Email _____

EXHIBIT "F" DATA SECURITY REQUIREMENTS (OPTIONAL)

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

00618-00001/4286742.1

Data Security

1. Security - Handling of Sensitive and Personal Information

a. Discuss and provide the servicer's information security policy, particularly as related to the program/product listed.

ManageBac servers are hosted on the iWeb data center in Montreal, Quebec (Canada). This secure facility is protected by the most modern access control in-use with dedicated facility management spaces. Our backups are hosted on an Amazon backup server and S3 secure buckets. We are hosted behind a Cisco ASA 5510 Sec+ hardware firewall. On the school end, we provide secure login and password requirements of over 8 characters, with numbers, symbols and capitalization required for each user. We provide different login access levels (determined by the school) for who has access to full student and teacher accounts (usually the head of school and IB coordinator only)

b. Describe the measures utilized by the service on identity theft.

In the unlikely event of identify theft, we immediately change the affected user's password and will work with the affected school to investigate the IP address to determine more about where the attack came from within 24 hours. We will also thoroughly review security protocols and best practices with the school administration to determine how the theft occurred (e.g. did the user leave their computer unsecured, etc).

c. Describe the servicer's policy with regard to the sale of customer information to commercial organizations, marketing films, or otherwise.

We do not ever sell customer information.

d. Describe the encryption standards that will be utilized for the transmission of data.

We use SSH encrypted connections for all data transfers and backups. All passwords and credit cards are encrypted using the MD5 hash format within our database. All production network traffic is encrypted with valid SSL Certificates.

e. Describe how your organization would handle any other fraud prevention and other security measures.

Within our own offices, all wi-fi networks are encrypted and passwords rotated regularly. We take every security precaution, including having school users verify their email addresses before any change is made, and ensuring all passwords are encrypted and have more than 8 characters. We work with schools to educate on best security practices during our training sessions.

f. How quickly can a determination be made as to whether data/files have been tampered with, or if the file-transfer security has been compromised?

Once notified, our development team responds to any vulnerabilities as soon as possible. At the latest, within 24 hours, but usually within the hour. We have never had a mass security breach in our system.

g. Describe the technical security architecture and how does the security architecture address data privacy and compliance concerns?

Our servers are hosted at the iWeb facility in Montreal, Quebec. Backups are hosted on an Amazon web server and S3 bucket to ensure data redundancy. We are fully hosted behind a CISCO firewall. For a full diagram of our architecture, please visit managebac.com/systems

2. **Security - Authentication via Single Sign-On (SSO)**

The Vendor must allow students and teachers access using a Single Sign-On (SSO) requirement of Security Assertion Markup Language 2.0 (SAML). SAML is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identify provider (Los Angeles Unified School District) and a service provider (Clever). The user management system must support Active Directory Federation Services (ADFS) in order to manage SSO accounts. The single most important SAML specification is Transport Layer Protection 1.2 to guarantee message confidentiality and integrity.

3. **Security - Data Management and Protection**

a. How does your service address the issues of data at rest and data in transit?

Data in transit is always encrypted with SSH Connections. All SSH connections use secure RSA public key authentication. The rest of our data is hosted on a physical server in Montreal with strict security protocols in place, behind a CISCO firewall.

b. What encryption and authentication mechanisms are employed with your servicing service? Describe the encryption algorithms/methodologies used, and how users are authorized and authenticated in the system.

Users are authorized and authenticated via email. Once a school administrator has been identified, it is their responsibility to send us a list of verified user emails. Once this list is in the system, we send secure emails (that expire within 24 hours) for the user to authenticate and set up their initial password.

c. Describe how the servicing system and/or individual program passwords are handled. What is the method of authentication?

Users are authorized and authenticated via email. Once a school administrator has been identified, it is their responsibility to verify

d. What are your password policies regarding password requirements/restrictions such as creation, expiration, forgotten password, etc.?

We require passwords to be longer than 8 characters with capitalization, numbers and symbols. Our recommendation (as written on all of our systems and tutorials) is for a secure 'pass phrase' of four words or longer. All password recreation/forgotten password links are emailed to the affected user and expire within 24 hours.

e. Describe your policy on backup and data retention.

All of our data is backed up regularly onto Amazon Servers and S3 buckets. All backup transfers occur on secure SSH connections, and we keep data for up to one year in case of deletion. Files are backed up every day. We also copy everything from our master storage to our slave DB server (backup server) in real time. That way the duplicate database can be brought online within 10 minutes with no data loss should the main server fail.

f. What logging, auditing, and reporting capabilities does your servicing services provide? Are audit trails available within the servicing system to list functions performed and by whom? What is the archival duration for audit trails? Who can delete audit trails? Describe the servicing services ability to audit transactions or maintain an audit trail for individual transactions. Elements might include posting date, modification dates, transaction changes, i.e. before and after images and user ID. Is there audit trail reporting available?

Yes, audit trails that list all user actions (including additions, deletions, posting dates, before and after images, IP addresses) are monitored by our development team, and these reports are available upon request from a school administrator within 1-2 business days. Our development team is the only group who has access to these trails. They are never deleted.

g. Describe your security incident responses and management methodologies and processes to expeditiously mitigate security breaches within your servicing services. What processes are in place for notification, escalation, and remediation?

We use Pingdom to monitor our servers and NewRelic/ScoutApp to monitor our application performance. If our server ever goes down or is breached, we immediately are notified via SMS and email alert to investigate the issue.

h. What is your institution practice on vulnerability assessment, identification, remediation and patch management practices?

All system installation uses patched OS Ubantu 14.04 LTS. We are assessed every year by the NCC Group to comply with IB requirements for security. All identified weak spots are sent to us immediately via SMS/email, and all our IP addresses are protected by CloudFlare to prevent vulnerabilities.

i. Do you outsource any services within domestic U.S. and/or outside of U.S. for the program/product listed? Describe what services are being outsourced and provide security measures taken.

We do not outsource any services. Our main server is in Canada (see more details above) in Quebec, but all monitoring of our system takes place by Faria Systems employees.

4. Security - User Protection and Restrictions

a. Is it possible to restrict users to a set list of programs or specific functions within an individual program? Yes ☑ No ☐
If yes, describe how these features work.

Yes, we provide several layers of user permissions. Admins have full access to everything in the system. Advisors have access to their own classes and students within those classes. Observers have access only to curriculum, in a read-only capacity. Students have access to their own work and calendars. Parents have access to their own student's records.

b. Is multi-factored authentication available? Yes ☑ No ☐
Describe the recommended practice with your service. Explain how access is provided.

Access is provided via email usernames and individual passwords. We are currently working towards multi-factored authentication for administrators.

c. Are additional or optional security features available? Yes ☐ No ☑
If yes, describe the options.

d. Describe input/process/output controls, and what types of secondary reviews are enabled to ensure separation of duties and date integrity.

Separattion of duties is the purview of the school administrators on ManageBac. They decide who gets full system access, and who gets limited access according to the user permission levels seen in question 4a.

e. Does your security support dual system administrator control? Yes ☑ No ☐
If yes, at what levels?

We at ManageBac are automatically given administrator access to school systems to assist with trainings, support and investigate any issues. School administrators are also given full access to the system and are in charge of setting up their own school Settings, subjects and permission levels.

f. Does the service allow for a master list of authorized signers by account?
If yes, describe the system security associated with maintaining and reviewing this list.

We provide a list of administrators via our Settings > School Directory > Admins lists. These lists are available to all administrators in the account and it is the responsibility of the school to maintain this list.

Also, who will be authorized to add/change/delete authorized signers and processes?

Anyone listed as a school administrator (usually the head of school or IB coordinator) in the system has the ability to add/edit/delete users.

g. Are you certified ISO 27001-2? Yes ☑ No ☐
If no, when will you be certified?