RHODE ISLAND STUDENT DATA PRIVACY AGREEMENT
VERSION MODIFIED (2020)

St. George's School

and

Naviance, Inc.

August 17

2020

This Rhode Island Student Data Privacy Agreement ("DPA") is entered into by and between the school district, St. George's School (hereinafter referred to as "LEA") and Naviance, Inc. (hereinafter referred to as "Provider") on August 17, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in Rhode Island the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq.; and

WHEREAS, the documents and data transferred from Rhode Island LEAs and created by the Provider's Services are also subject to several Rhode Island student privacy laws, including R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

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 (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described in Exhibit "A".

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and Exhibit "A", LEA shall provide the categories of data described 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 terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to this 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 or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, 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. LEA may access its Student Data by using the controls available to it in the Services. If Provider offers separate accounts for pupils, Provider may transfer pupil-generated content to a separate pupil 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 personally identifiable information on 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. LEA may use existing functionality in Provider services to access, amend and correct those records. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of 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**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account if Provider offers such accounts.

4. **Third Party Request**. Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, 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 unless legally prohibited from doing so, and shall reasonably cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not sell or allow any other third party or entity to sell Student Data or any portion thereof. Provider will not use, disclose, compile or transfer Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile or transfer Student Data and/or any portion thereof, except

as necessary to provide the Services, without the express written consent of the LEA or without a court order or lawfully issued subpoena. 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.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq., and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."

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

3. **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 Rhode Island and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as 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, any student data, 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, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

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 this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.

4. **No Disclosure**. De-identified information, as defined in Exhibit "C", may be used by the Provider for the purposes of development, research, demonstrating the efficacy of its products, 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). The Provider and LEA agree that the Provider may not disclose information if there are fewer than twenty (20) students in the samples of a particular field or category of information collected, i.e., twenty students in a particular grade, twenty students of a particular race, or twenty students with a particular disability. 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 the LEA who has provided prior written consent for such transfer. The prior sentence does not apply to Subprocessors whom the Provider uses to assist in providing the services outlined in this DPA or whom the Provider uses to assist for the purposes of development, research, and improvement of educational sites, services, or applications. Provider shall not copy, reproduce or transmit any data obtained under this DPA and/or any portion thereof, except as authorized by the DPA.

5. **Disposition of Data**. Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained As soon as practicable upon expiration or termination of the service agreement, but in any event no later than six (6) months after expiration or termination, Provider will delete personally identifiable student information. Notwithstanding the above, LEA may, at any time and in its sole discretion, request in writing that its personally identifiable student information be deleted, and Provider shall comply with any such written request within thirty (30) days. Nothing in this DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Upon receipt of written request from LEA for confirmation of disposition of Student Data, Provider shall provide written notification within a reasonable time frame. 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. LEA may at any time during the term of service download a copy of Student Data.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or

advertising 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 Client; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client. LEA agrees that the Services provided as outlined in Exhibit "A" are acceptable. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standard 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 and establish authentication to protect access to Student Data, at a level suggested by 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 pass criminal background checks.

    b. **Destruction of Data**. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained and make available said data to LEA, in a readable and usable format. Nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

    c. **Security Protocols**. Both parties agree to maintain security protocols that meet standard industry practices 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 DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

    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, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data

from unauthorized access. The service security measures shall include server authentication and data encryption, at rest and in transit. Provider shall host data pursuant to the DPA in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.

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 periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

j. **Audits.** Once a year upon the LEA's written request and execution of a nondisclosure agreement, Provider will give the LEA a copy of the Providers SOC2 report. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within three (3) days of the incident. 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 Provider 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, including the number of affected individuals and how the security breach occurred.

vi. Information about remediation efforts conducted by the Provider to contain and mitigate the breach.

vii. If required by applicable law, toll free numbers and websites to contact:

1. The credit reporting agencies
2. Remediation service providers
3. The attorney general

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

iii. A clear and concise description of the affected parent, legal guardian, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

b. Provider agrees to adhere to all requirements in 11-49.3-1, et. seq. and in federal law with respect to a data breach related to the Student Data, including, when required, the required responsibilities and procedures for notification and mitigation of any such data breach.

c. Provider further acknowledges and agrees to have a written incident response plan that reflects standard 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 written request and a signed non-disclosure agreement, with a copy of said written incident response plan.

d. At the request and with the assistance of the District, 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.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Parties shall be bound by this DPA for the duration of the Service agreement or for 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 and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any material terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the applicable privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other 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, facsimile 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 below.

The designated representative for the Provider for this Agreement is:

Name	Monica Morrell
Title	Sr. Vice President, Customer Experience
Address	3033 Wilson Blvd, Suite 500, Arlington, VA 22201
Telephone Number	703-859-7367
Email	monica.morrell@hobsons.com

The designated representative for the LEA for this Agreement is:

Name	Robyn B. Cavanagh
Title	Director of Technology
Address	372 Purgatory Rd. Middletwon, RI
Telephone Number	(401) 8426740
Email	robyn_cavanagh@stgeorges.edu

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 RHODE ISLAND, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF [COUNTY OF LEA] COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA 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.

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. **Electronic Signature:** The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with Rhode Island and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate

the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

ARTICLE VII- GENERAL OFFER OF 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 to any other school district who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

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

St. George's School

By: Robyn B. Cavanagh Date: Sep 21, 2020

Robyn B. Cavanagh (Sep 21, 2020 14:35 EDT)

Printed Name: Robyn B. Cavanagh Title/Position: Director of Technology

Naviance, Inc.

By: Monica L Morrell Date: June 16, 2020

Printed Name: Monica Morrell Title/Position: SVP, Customer Experience

EXHIBIT "A"

DESCRIPTION OF SERVICES

The Service is a web and mobile-based college and career readiness platform that helps students explore goal setting, academic planning, career exploration, and college and related postsecondary education preparation and planning. The Service also helps to identify and facilitate student connection with higher education institutions and scholarship providers that are of interest, while simultaneously operating as the system of records for Customers. Many core features of the Service may be activated solely at the discretion of Customer.

The Service also includes a browser interface and data transmission, access, storage (subject to commercially reasonable limits as may be imposed by Naviance in its sole discretion) and single sign-on capabilities. Customers and Users are responsible for their own Internet connection, communications and computer costs.

Matching Features. The college planning function contained in the Service includes certain optional features (collectively, "Matching") that allow students to view information from and interact with Hobsons' higher education Intersect subscribers ("Higher Education Institutions"). Matching is inactive by default, and therefore must be enabled by an authorized representative of Customer who has obtained consent from the student's parent or legal guardian prior to at the activation of Matching. Matching may be turned on or off at any time of the sole discretion and control of Customer.

If Customer enables Matching for its students, its students will be able to:

View supplemental material on college profile pages and upcoming informational and other pre-enrollment events, and RSVP to upcoming events hosted by Higher Education Institutions.

In addition, students who meet certain non-personally identifiable criteria will:

Receive additional information about nonprofit Higher Education Institutions, and if a student expresses interest in a nonprofit Higher Education Institution, that the student will receive an invitation through the Service to connect directly with the Higher Education Institution. The student may then choose either to disregard or to respond to the invitation.

No student or Customer information is shared with any Higher Education Institution unless Customer has enabled Matching and the applicable student has explicitly opted to send his/her information directly to the Higher Education Institution.

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.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	X
	Observation data	NA
	Other assessment data-Please specify:	X
Attendance	Student school (daily) attendance data	NA
	Student class attendance data	NA
Communications	Online communications that are captured (emails, blog entries)	Email sent in Naviance
Conduct	Conduct or behavioral data	NA
Demographics	Date of Birth	X
	Place of Birth	NA
	Gender	X
	Ethnicity or race	BOTH
	Language information (native, preferred or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	NA
	Teacher names	X
Special Indicator	English language learner information	Handled through student groups
	Low income status	Handled through student groups
	Medical alerts	NA
	Student disability information	Handled through student groups
	Specialized education services (IEP or 504)	Handled through student groups
	Living situations (homeless/foster care)	Handled through student groups
	Other indicator information-Please specify:	First generation
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Student app username	X
	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 program-student reads below grade level)	NA
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X student enter
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures etc.	X
	Other student work data - Please specify:	X

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	X
	Other transcript data -Please specify:	
Transportation	Student bus assignment	NA
	Student pick up and/or drop off location	NA

Category of Data	Elements	Check if used by your system
	Student bus card ID number	X
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider 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. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual. De-identified information cannot be disclosed if there are fewer than twenty (20) students in the samples of a particular field or category, i.e., twenty students in a particular grade or less than twenty students with a particular disability.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

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 that identifies an individual. PII includes, without limitation, at least the following:

(a) The student's name.
(b) The name of the student's parents or other family members.
(c) The address of the student or student's family.
(d) Indirect identifiers, including the student's date of birth, place of birth, social security number, email, social media address, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number.
(e) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

Provider: For purposes of the DPA, 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.

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 local educational LEA employee.

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 Rhode Island 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.

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its 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 an entity that is not the provider or LEA.

OPTIONAL: EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? □ Yes □ No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

____ CIS Critical Security Controls

____ NIST Framework for Improving Critical Infrastructure Security

____ Other: _____

3. Does your organization store any customer data outside the United States? □ Yes □ No

B. 4. Does your organization encrypt customer data both in transit and at rest? □ Yes □ No

C. 5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: _____

Contact information: _____

D. 6. Please provide any additional information that you desire.

St.georges_ri_naviance

Final Audit Report 2020-09-21

Created:	2020-08-18
By:	Chrystal Hoe (choe@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAf0FdCWHscyr8eGDfHP5dmZ-NM7fktnLu

"St.georges_ri_naviance" History

Document created by Chrystal Hoe (choe@tec-coop.org)
2020-08-18 - 1:58:12 AM GMT- IP address: 72.134.43.11

Document emailed to Robyn B. Cavanagh (robyn_cavanagh@stgeorges.edu) for signature
2020-08-18 - 1:58:47 AM GMT

Email viewed by Robyn B. Cavanagh (robyn_cavanagh@stgeorges.edu)
2020-08-18 - 10:14:50 AM GMT- IP address: 66.102.8.111

Email viewed by Robyn B. Cavanagh (robyn_cavanagh@stgeorges.edu)
2020-09-21 - 6:34:35 PM GMT- IP address: 66.102.8.96

Document e-signed by Robyn B. Cavanagh (robyn_cavanagh@stgeorges.edu)
Signature Date: 2020-09-21 - 6:35:44 PM GMT - Time Source: server- IP address: 131.109.17.2

Agreement completed.
2020-09-21 - 6:35:44 PM GMT