Agreement #SA-1819-XXX-XX
Approved: _____

**EXHIBIT "B"**

**DATA SHARING AND PRIVACY AGREEMENT**

**BETWEEN**

**THE SCHOOL BOARD OF SEMINOLE COUNTY, FLORIDA**

and

_____
**CONTRACTOR NAME**

_____

Term (Maximum of 3 Years):

Start Date: _____

End Date: _____

Administrator Responsible: _____
Printed Name / Title

This Data Sharing and Privacy Agreement ("DSPA") is entered into by and between the School Board of Seminole County, Florida (hereinafter referred to as "SBSC") and _____ (hereinafter referred to as "Contractor") on _____. The Parties agree to the terms as stated herein.

**RECITALS**

**WHEREAS,** the Contractor has agreed to provide ("SBSC") with certain digital educational services ("Services") pursuant to a Services Agreement # _____ ("Service Agreement"); and

**WHEREAS,** in order to provide the Services described in the Service Agreement, the Contractor may receive and the SBSC 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"), at 15 U.S.C. 6501-6506 (16 CFR Part 312), and Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and

**WHEREAS,** the documents and data transferred from SBSC and/or accessed by the Contractor in the performance of the Services Agreement are also subject to state privacy laws; and

**WHEREAS**, this Agreement complies with Florida Statutes Sections 1001.41 and 1002.22 and Federal laws; and

**WHEREAS**, the Parties wish to enter into this DSPA to ensure that accessing and/or transferring of data resulting from the performance of the Services Agreement complies with the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

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

**ARTICLE I: PURPOSE AND SCOPE**

1. **Purpose of DSPA**. For Contractor to provide services to the SBSC it may become necessary for the SBSC to share certain Data related to the SBSC's students, employees, business practices, and/or intellectual property. This agreement describes responsibilities to protect Data between the SBSC and Contractor.

2. **Nature of Services Provided**. The Contractor has agreed to provide the following digital educational services described below and as may be further outlined in [Cite section of Service Agreement] hereto:

3. **Data to Be Provided**. In order to perform the Services described in the Service Agreement, SBSC shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Attachment "1".

4. **DSPA Definitions**. The definitions of terms used in this DSPA are found in Attachment "2".

**ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Data Property of SBSC**. All Data transmitted to the Contractor pursuant to the Service Agreement is and will continue to be the property of and under the control of the SBSC. The Contractor further acknowledges and agrees that all copies of such Data transmitted to the Contractor, 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 Data. The Parties agree that as between them all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the SBSC. For the purposes of FERPA and Pursuant to 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii), the Contractor will provide to SBSC the specified services the SBSC could otherwise use its employees to perform. Contractor agrees that for purposes of this Agreement, it will be designated a "School Official," under the control and direction of the SBSC as it pertains to the use of data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. Contractor may transfer student-generated content to a separate account, according to the procedures

set forth below. Contractor agrees to abide by FERPA and Fla. Stat. 1002.22 while performing its service for the SBSC.

2. **Parent Access**. SBSC shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the student's records. Contractor shall respond in a reasonably timely manner (and no less than 10 days from the date of request) to the SBSC's request for Data in a student's records held by the Contractor to view or correct as necessary. In the event that a parent of a student or other individual contacts the Contractor to review any of the Data accessed pursuant to the Services, the Contractor shall refer the parent or individual to the SBSC, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Contractor shall, at the request of the SBSC, transfer Student-Generated Content to a separate student account.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Contractor with a request for data held by the Contractor pursuant to the Services, the Contractor shall redirect the Third Party to request the data directly from the SBSC. Contractor shall notify the SBSC in advance of a compelled disclosure to a Third Party. The Contractor will not use, disclose, compile, transfer, or sell the 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, transfer or sell the Data and/or any portion thereof.

5. **No Unauthorized Use**. Contractor shall not use Data for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Contractor shall enter into written agreements with all Subprocessors, listed in Attachment "4"**,** performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Data in a manner consistent with the terms of this DSPA.

## ARTICLE III: DUTIES OF SBSC

1. **Provide Data In Compliance With State and Federal Law**. SBSC will allow Contractor access to data necessary to perform the services pursuant to the Services Agreement and pursuant to the terms of this DSPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DSPA.

2. **Annual Notification of Rights.** If the SBSC has a policy of disclosing education records under 34 CFR § 99.31 (a) (1), SBSC 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, and determine whether Contractor qualifies as a school official.

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

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

## ARTICLE IV: DUTIES OF CONTRACTOR

1. **Privacy Compliance**. The Parties expect and anticipate that Contractor may receive personally identifiable information in education records from the District only as an incident of service or training that Contractor provides to the SBSC pursuant to this Agreement. The Contractor shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this DSPA. The Parties agree that Contractor is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Contractor: (1) provides a service or function for which the SBSC would otherwise use employees; (2) is under the direct control of the SBSC with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records

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. Contractor also acknowledges and agrees that it shall not make any re-disclosure of any 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 Data, without the express written consent of the SBSC.

3. **Employee Obligation**. Contractor shall require all employees and agents who have access to Data to comply with all applicable provisions of this DSPA with respect to the data shared under the Service Agreement. Contractor agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.

4. **No Disclosure**. Contractor may use aggregate data only 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). Contractor agrees not to attempt to re-identify de-identified Data and not to transfer de-identified 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 SBSC who has provided prior written consent for such transfer. Contractor 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**. Contractor shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to SBSC or SBSC's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Contractor to maintain Data obtained under the Service Agreement beyond the time-period reasonably needed to complete the disposition. Disposition shall include:

   a. (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to SBSC when the Data has been disposed of. The duty to dispose of 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 DSPA. The SBSC may employ a "Directive For Disposition of Data", a copy of which is attached hereto as Attachment "3". Upon receipt of a request from the SBSC, the Contractor will immediately provide the SBSC with any specified portion of the Data within three (3) calendar days of receipt of said request.

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

7. **Access to Data**. Contractor shall make Data in the possession of the Contractor available to the SBSC within five (5) business days of a request by the SBSC.

## ARTICLE V: DATA PROVISIONS

1. **Data Security** . The Contractor agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Contractor are set forth below. Contractor may further detail its security programs and measures in Attachment 4 hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Contractor shall secure usernames, passwords, and any other means of gaining access to the Services or to Data by using a form of multi-factor authentication (MFA) at a minimum level equivalent to the level delineated in Article 4.3 of NIST 800-63-3. Contractor shall only provide access to Data to employees or contractors that are performing the Services.

   b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best 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. Contractor shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer 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 SBSC.

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

**d.** **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. Contractor shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

**e.** **Security Coordinator**. Contractor shall provide the name and contact information of Contractor's Security Coordinator for the Data received pursuant to the Service Agreement, pursuant to Attachment "4".

**f.** **Subprocessors Bound**. Contractor may enter into written agreements whereby Subprocessors, listed in Attachment "4" agree to secure and protect Data in a manner consistent with the terms of this Article V. Contractor shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

**g.** **Periodic Risk Assessment**. Contractor further agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Contractor will provide the SBSC with the results of the above risk assessments and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DSPA.

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

**i.** **Audits.** Upon receipt of a request from the SBSC, the Contractor will allow the SBSC to audit the security and privacy measures that are in place to ensure protection of the Data. The Contractor will cooperate fully with the SBSC and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Contractor and/or delivery of Services to students and/or SBSC, and shall provide full access to the Contractor's facilities, staff, agents and SBSC's Data and all records pertaining to the Contractor, SBSC and delivery of Services to the Contractor. Failure to cooperate shall be deemed a material breach of the DSPA.

**2.** **Data Confidentiality -** Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Protected Information including Personally Identifiable Information (PII), protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to SBSC or an individual identified with the data or information in Contractor's custody.

a. Contractor certifies that it has implemented policies and procedures to protect against reasonably foreseeable unauthorized access to, or disclosure of, District Data or PII, and to prevent other reasonably foreseeable events that may result in substantial harm to District or any individual student identified in such PII.

b. Contractor shall not permit District Data or PII to be maintained or stored on any Mobile Device or Portable Storage Medium unless such is being used in connection with Vendor's backup and recovery procedures and/or encrypted

c. Contractor shall not, without the express prior written consent of District:
   - Maintain or store District Data or PII outside of the United States,
   - Transmit District's Data or PII to any contractors or subcontractors located outside of the United States,
   - Distribute, repurpose or share District Data or PII with any Partner Systems not used for providing services to the District,

- Use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes],
- Use PII or any portion thereof to develop commercial products or services,
- Use any PII for any other purpose other than in connection with the services provided to the District,
- Engage in targeted advertising, based on the data collected from the District

**3.** **Data Breach**. Contractor certifies that it has implemented policies and procedures addressing a potential Security Breach and that it possesses an up to date Security Breach response plan. Such plan shall be made available, upon request, to the District.

Contractor shall comply with all applicable federal and state laws that require notification to individuals, entities, state agencies, or federal agencies in the event of a Security Breach including the State of Florida Database Breach Notification process.

Contractor agrees to comply with the State of Florida Database Breach Notification process and all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), Contractor agrees to notify SBSC immediately and to indemnify, hold harmless, and defend SBSC and its officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

**4.** When Contractor reasonably suspects and/or becomes aware of a disclosure or security breach concerning any Data covered by this Agreement, Contractor shall notify the SBSC immediately and mitigate the damage of such security breach to the greatest extent possible.

**a.** Subject to the following requirements, the Contractor shall provide a security breach notification to the SBSC.

**i.** 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.

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

**1)** The name and contact information of the reporting individual subject to this section.
**2)** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
**3)** 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.
**4)** 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.
**5)** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

**iii.** The security breach notification must include at least:

**1)** Information about what the Contractor has done to protect individuals whose information has been breached.
**2)** Advice on steps that the person whose information has been breached may take to protect himself or herself.
**3)** Information about the steps the Contractor has taken to cure the breach and the estimated timeframe for such cure.

**b.** Contractor agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

**c.** Contractor further 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 Data or any portion thereof, including personally identifiable information and agrees to provide SBSC, upon request, with a copy of said written incident response plan.

**d.** Contractor further agrees that it will provide the notification directly to SBSC and will fully cooperate, and assist as specifically requested by SBSC, with all efforts by the SBSC to notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsection (a) above.

**e.** The Parties agree that any breach of the privacy and/or confidentiality obligation set forth in the DSPA may, at the SBSC's discretion, result in the SBSC immediately terminating the Service Agreement and any other agreement for goods and services with Contractor. Termination does not absolve the Contractor's responsibility to comply with the disposition procedures of Data.

## ARTICLE VI: MISCELLANEOUS

1. **Term**. The Contractor shall be bound by this DSPA for the duration of the Service Agreement or so long as the Contractor maintains any Data. Notwithstanding the foregoing, Contractor agrees to be bound by the terms and obligations of this DSPA for no less than three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DSPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Contractor shall dispose of all of SBSC's Data pursuant to Article IV, section 5.

4. **Priority of Agreements**. This DSPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DSPA.

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 before:

   The designated representative for the Contractor for this Agreement is:

   _____
   _____
   _____
   _____
   _____

   The designated representative for the SBSC for this Agreement is:

   _____
   _____
   _____
   _____
   _____

6. **Severability**. Any provision of this DSPA 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 DSPA, 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 DSPA or affecting the validity or enforceability of such provision in any other jurisdiction.

7. **Authority**. Contractor represents that it is authorized to bind to the terms of this DSPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.

8. **Waiver**. Waiver by any party to this DSPA of any breach of any provision of this DSPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DSPA shall not operate as a waiver of such right. All rights and remedies provided for in this DSPA are cumulative. Nothing in this DSPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the SBSC, its officers, employees, and agents as a result of the execution of this DSPA or performance of the functions or obligations described herein.

9. **Assignment**. None of the parties to this DSPA may assign their rights, duties, or obligations under this DSPA, either in whole or in part, without the prior written consent of the other party to this DSPA.

[*Signature Page Follows*]

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

**CONTRACTOR:** _____

BY:_____ Date:_____

Printed Name:_____ Title/Position:_____

Address for Notice Purposes: _____

**SBSC:** _____

BY:_____ Date:_____

Printed Name:_____ Title/Position:_____

Address for Notice Purposes: _____

**Attachment "1"**

**SCHEDULE OF DATA**

| Category of Data | Elements | Initial if used by your system |
|---|---|---|
| Application Technology Meta Data | IP Addresses of users, Use of cookies etc. | |
| Application Technology Meta Data | Other application technology meta data Please specify:<br>*<br>*<br>*<br>* | |
| Application Use Statistics | Meta data on user interaction with application | |
| Assessment | Standardized test scores | |
| Assessment | Observation data | |
| Assessment | Other assessment data<br>Please specify:<br>*<br>*<br>*<br>* | |
| Attendance | Student school (daily) attendance data | |
| Attendance | Student class attendance data | |
| Communication | Online communications that are captured (emails, blog entries) | |
| Conduct | Conduct or behavioral data | |
| Demographics | Date of Birth | |
| Demographics | Place of Birth | |
| Demographics | Gender | |
| Demographics | Ethnicity or race | |
| Demographics | Specialized education services (IEP or 504) | |
| Demographics | Living situations (homeless/foster care) | |
| Demographics | Language information (native, preferred or primary language spoken by student) | |
| Demographics | Other indicator information<br>Please specify:<br>*<br>*<br>*<br>* | |
| Enrollment | Student school enrollment | |
| Enrollment | Student grade level | |
| Enrollment | Homeroom | |
| Enrollment | Guidance counselor | |
| Enrollment | Specific curriculum programs | |
| Enrollment | Year of graduation | |
| Enrollment | Other enrollment information<br>Please specify:<br>*<br>*<br>*<br>* | |
| | | |

| Category of Data | Elements | Initial if used by your system |
|---|---|---|
| Parent/Guardian Contact Information | Address | |
| Parent/Guardian Contact Information | Email | |
| Parent/Guardian Contact Information | Phone | |
| Parent/Guardian Name | First and/or Last | |
| Schedule | Student scheduled courses | |
| Schedule | Teacher names | |
| Special Indicator | English language learner information | |
| Special Indicator | Low income status - SES Free and Reduced | |
| Special Indicator | Medical alerts/health data | |
| Special Indicator | Student disability information | |
| Student Contact Information | Address | |
| Student Contact Information | Email | |
| Student Contact Information | Phone | |
| Student Identifiers | Local (School district) ID number | |
| Student Identifiers | Vendor/App assigned student ID number | |
| Student Identifiers | Student app username | |
| Student Identifiers | Student app passwords encrypted only for SSO | |
| Student Name | First and/or Last | |
| Student In App Performance | Program / application performance (typing program- student types 60 wpm, reading program-student reads below grade level) | |
| Student Survey Responses | Student responses to surveys or questionnaires | |
| Student work | Student generated content; writing, pictures etc. | |
| Student work | Other student work data<br>Please specify:<br>*<br>*<br>*<br>* | |
| Transcript | Student course grades | |
| Transcript | Student course data | |
| Transcript | Student course grades/performance scores | |
| Transcript | Other transcript data<br>Please specify:<br>*<br>*<br>*<br>* | |
| Transportation | Other transportation data<br>Please specify:<br>*<br>*<br>*<br>* | |

| Category of Data | Elements | Initial if used by your system |
|---|---|---|
| Other | Please list each additional data element used, stored or collected through the services defined in Exhibit A | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |
| Other | | |

**Attachment "2"**

**DEFINITIONS**

**Contractor:** The term "Contractor" means the Contractor 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. This term shall encompass the term "Third Party," as it is found in applicable statutes.

**Data:** Data shall include, but is not limited to, the following: student data, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Florida and Federal laws and regulations. Data as specified in Attachment "1" is confirmed to be collected or processed by the Contractor pursuant to the Services.

**Data Destruction:** Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

**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 DSPA, Educational Records are referred to as Data.

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

**Personally Identifiable Information (PII):** includes but is not limited to: personal identifiers such as name, address, phone number, dates of birth, Social Security number, and student or personnel identification number; "personal information student records", personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act ("FERPA"), 20 UCS §1232g; "protected health information" as the term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; "nonpublic personal information" as the term is defined in the Gramm-Leach-Bailey Financial Modernization Act of 1999, 15 USC §6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state-or federal identification numbers such as passport, visa or state identify card numbers; and "covered information". In addition, Personally Identifiable Information" or PII" shall include, but are not limited to, Data, metadata, and user or student-generated content obtained by reason of the use of Contractor's software, website, serve, or app, including mobile apps, whether gathered by Contractor or provided by SBSC or its users, students, or students' parents/guardians, includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow reasonable persons to be able to identify a student to a reasonable certainty. For purposes of this DSPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

**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.

**Service Agreement**: Refers to the Contract or Purchase Order that this DSPA supplements and modifies.

**Student -Generated Content:** The term "student-generated content" means materials or content created by a student 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 student content.

**Student Records:** Means both of the following: (1) Any information that directly relates to a student that is maintained by SBSC and (2) any information acquired directly from the student through the use of instructional software or applications assigned to the student by a teacher or other SBSC employee. For the purposes of this Agreement, student Records shall be the same as Educational Records.

**Subprocessor:** For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than SBSC or Contractor, who Contractor 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 Contractor'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 student 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 "Contractor."

**Attachment "3"**

**DIRECTIVE FOR DISPOSITION OF DATA**

_____ directs _____ to dispose of data obtained by Company pursuant to the terms of the Service Agreement between SBSC and Company. The terms of the Disposition are set forth below:

1. Extent of Disposition

____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

_____

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

___ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

3. Timing of Disposition

Data shall be disposed of by the following date:

___As soon as commercially practicable

___By _____

4. Signature

_____ _____
Authorized Representative of SBSC Date

5. Verification of Disposed Data

_____ _____
Authorized Representative of Company Date

**Attachment "4"**

**DATA SECURITY**

1. **Security Coordinator Information:**

Named Security Coordinator

Email of Security Coordinator

Phone Number of Security Coordinator

2. **Subprocessor List:**

3. **Additional Data Security Requirements:**