**DATA SHARING ADDENDUM BETWEEN THE DISTRICT AND BRIGHTBYTES, INC.**

This Data Sharing and Processing Addendum (“**Addendum**”) is hereby attached to and incorporated into the Order Form entered between \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(“**District**”) and BrightBytes, Inc., a Delaware corporation (“**BrightBytes**” and together with District, the “**Parties**”), and hereby made a part of the Agreement (as defined in the Sales Order Form) between the Parties. Terms which are not defined herein have meaning in the Sales Order Form (*See* Attachment “A”) or the Terms of Service (*See* Attachment “B”) or the Privacy Statement (*See* Attachment “F”), as applicable. To the extent the terms in this Addendum conflict with the Terms of Service, Privacy Statement, or any other attachment or exhibit, the Addendum will govern to the extent of the conflict and to the exclusion of those terms in any other attachment or contractual document. This Addendum changes the Terms of Service (*See* Attachment “B”), Data Integration Specification (*See* Attachment “C”), and the Privacy Statement (*See* Attachment “F”).

1. **Purpose and Scope:** This agreement is entered into by District and BrightBytes solely and exclusively for the purpose of sharing information between the Parties, and with the Mississippi Department of Education (“MDE”), in accordance with the assurances made by the District by and through its participation in the Mississippi Connects Digital Learning Program under the Equity in Distance Learning Act (EDLA). Through the EDLA districts agreed to participate in data collection regarding the performance and effectiveness of district’s digital learning program. This data collection will be provided through the BrightBytes EdTech Impact platform. In addition, data collection through the BrightBytes Progress Monitoring platform will use the same data collection for EdTech Impact to help districts 1) monitor student growth on local and state assessments, and 2) determine the effectiveness of in-person and virtual learning environments.   Access to the BrightByes Progress Monitoring platform will be available to District and in limited view, to MDE, pursuant to the Agreement. Specifically, MDE will have limited access to school and district level student data in aggregate form. The BrightBytes EdTech Impact platform and Progress Monitoring platform are collectively referred to as “Service(s)” in this Addendum.

This Addendum describes the duties and responsibilities to protect student data transmitted to BrightBytes from the District pursuant to the Agreement, including compliance with the Federal Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. § 1232(g), the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. §§ 6501-6502; the Protection of Pupil Rights Amendment (“PPRA”), 20 U.S.C. § 1232, and other applicable laws, rules and best practices relating to the protection of the personal information of students. In performing the Service, and for the limited purpose thereof, BrightBytes shall be considered a School Official with a legitimate educational interest.

Pursuant to FERPA, 20 U.S.C. § 1232(g), and the FERPA regulations that took effect January 8, 2009:

An educational agency or institution may disclose personally identifiable information from an educational record of a student without the consent required by § 99.30, if the disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. 34 C.F.R. § 99.31(a)(6)(i)

Additionally, as set forth in 34 C.F.R. § 99.31(a)(6)(iii):

An educational agency or institution may disclose personally identifiable information under paragraph (a)(6)(i) of this section, and a State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section may redisclose personally identifiable information under paragraph (a)(6)(i) and (a)(6)(ii) of this section, only if:

* 1. The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;
  2. The information is destroyed when no longer needed for the purposes for which the study was conducted; and
  3. The educational agency or institution or the State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section enters into a written agreement with the organization that—
     1. Specifies the purpose, scope, and duration of the study or studies and the information to be disclosed;
     2. Requires the organization to use personally identifiable information from education records only to meet the purpose or purposes of the study as stated in the written agreement;
     3. Requires the organization to conduct the study in a manner that does not permit personal identification of parents and students, as defined in this part, by anyone other than representatives of the organization with legitimate interests; and
     4. Requires the organization to destroy all personally identifiable information when the information is no longer needed for the purposes for which the study was conducted and specifies the time in which the information must be destroyed.

This DSA establishes the terms, conditions, and limitations on the use of data provided to BrightBytes by the District for the purpose described above. Attachment C defines the data, including but not limited to personally identifiable information (“PII”), covered by this DSA. BrightBytes represents and warrants that the data identified in Attachment “C” (hereinafter referred to as District Data) is limited to that which is absolutely necessary for BrightBytes to prepare the reports to MDE as set out in Attachment “D.” The District shall not be obligated to transmit, provide, or otherwise send BrightBytes any data outside of that listed in Attachment “C.” The BrightBytes EdTech Impact Solution and Progress Monitoring Platform will not scrape, gather, or otherwise collect from the District any data outside of that listed in Attachment “C.” For avoidance of doubt, the foregoing prohibition does not apply to any Google products or services used by District or users of other BrightBytes products or services. Nothing in this DSA shall preclude the District and BrightBytes from entering into a separate, independent agreement for the provision of additional services, or the sharing of data for additional purposes. Attachment “D” defines the data, aggregated at the school and district level (no PII) covered by this DSA that will be transferred from BrightBytes to the MDE. Only data identified in Attachment “D” will be released from BrightBytes and transferred to MDE.

1. **Definitions:** As used in this DSA -

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations and reauthorization when effective. Nothing in this Agreement may be construed to allow either party to maintain, use, disclose or share student information in a manner not allowed by federal law or regulation.

In accordance with FERPA, 34 C.F.R. § 99.3, "Personally Identifiable Information" or "PII" includes but is not limited to:

1. The student's name;
2. The name of the student's parent or other family members;
3. The address of the student or student's family;
4. A personal identifier, such as the student's social security number, student number, or biometric record;
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. 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; or
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

"Destroy" or "Destruction" means the act of ensuring that data cannot be reused or reconstituted in a format that could be used as originally intended and that the data is impossible to recover or reconstitute in its original format.

“De-identified data” means records and information from which all personally identifiable information and has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including but not limited to, any information that, alone or in combination is linkable to a specific student taking in account reasonable available information.

“Data Breach” means the unauthorized release, access, disclosure, or acquisition of data that compromises the security, confidentiality, or integrity of data maintained by BrightBytes.

“IDEA” means the Individuals with Disabilities Education Act of 2004 (codified at 20 U.S.C. §§ 1400 et seq.) and includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapter 300 of Title 34 of the Code of Federal Regulations and reauthorization when effective. Nothing in this Agreement may be construed to allow either party to maintain, use, disclose or share student information in a manner not allowed by federal law or regulation.

Under IDEA, Destruction means physical destruction or removal of personal identifiers from information so that the information is no longer personally identifiable. 34 C.F.R. § 300.611.

In accordance with IDEA, 34 C.F.R. § 300.32, "Personally Identifiable Information" or "PII" includes but is not limited to:

1. The name of the child, the child’s parent, or other family member;
2. The address of the child;
3. A personal identifier, such as the child’s social security number or student number; or
4. A list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty.

“Student Data” is any personal information that is directly related to an identifiable current or former student that is maintained by BrightBytes on the District’s behalf pursuant to this Agreement. For clarity and without limitation, “Student Data” includes “personally identifiable information” or “PII” as those terms are defined by FERPA and IDEA.

THEREFORE, in consideration of the mutual understanding and agreement set forth, the **District** and **BrightBytes** do hereby agree to the following:

# Scope of Services:

1. **Both District and BrightBytes agree:**
   1. To maintain confidentiality of all education records as required under FERPA, IDEA, and other state and federal laws and regulations.
   2. To maintain safeguards that restrict the release or disclosure of information exchanged under this DSA as required under federal and/or state law or regulations related to data protection, data analysis, and the confidentiality of student information.
   3. That all copies of data of any type, including any modifications or additions to data from any source that contain PII, are subject to the provisions of this DSA in the same manner as the original data.
   4. That the Student Data to be transferred under this DSA from the BrightBytes to the MDE have been received from third parties (i.e., District) without a means by which to determine the accuracy of the data.
   5. Ownership and Control. BrightBytes shall access and process Student Data solely for the purposes of providing an outsourced institutional function pursuant to FERPA 34 C.F.R Part 99.31(a)(1). As between BrightBytes and the District, the District owns all right, title, and interest to all Student Data provided or otherwise made available to BrightBytes. The transfer of District Data from District to BrightBytes does not constitute a transfer of ownership of data or create an ownership interest on the part of BrightBytes in the data elements, analysis of the data, or any aggregate data contained in reports created from District Data, except to provide the Services described herein. Both parties agree to uphold their responsibilities under laws governing the privacy of Student Data, including in the U.S. the Family Educational Rights and Privacy Act ("**FERPA**"), the Protection of Pupil Rights Amendment (“**PPRA**”), and the Children's Online Privacy and Protection Act ("**COPPA**"), as applicable. BrightBytes will rely on District to obtain and provide appropriate consent and disclosures, if necessary, for BrightBytes to collect any Student Data, including the collection of Student Data directly from students under 13, as permitted under COPPA.
   6. BrightBytes does not have permission to redisclose District Data to a third party except upon prior written authorization of the District Superintendent or his or her designee, or to the MDE (except as contemplated under this Agreement), as a required part of this Addendum as provided in the assurances signed by the District related to its participation in the Equity in Distance Learning Act. Notwithstanding the foregoing, nothing in this agreement shall prohibit BrightBytes from disclosing District Data to vendors, contractors, sub-processors or affiliates, provided that such recipients are bound by contractual agreements to protect District Data in a manner no less stringent than the terms of this DSA. For clarity, authorized users of the District who access the BrightBytes services pursuant to the Agreement shall not be “third parties” for purposes of this Section
   7. That any transmission, transportation, processing, use, or storage of District data outside the United States is prohibited except upon prior written authorization of the District Superintendent or her designee. For avoidance of doubt, BrightBytes may use the services of its personnel located outside of the United States to perform its obligations under the Agreement, all of whom shall be subjected to the confidentiality obligations set forth in Section 3(b)(1) below.
   8. That the Director of BrightBytes, or their designee, and the District’s Chief Information Officer, or their designee, will make commercially reasonable efforts to review the provisions of this DSA annually to assure that the parties are acting in compliance with the requirements of this DSA. If any data security problems are identified, a report specifying problems, solutions, and timelines for implementation will be developed cooperatively with personnel from all Parties.

# BrightBytes Agrees:

* 1. Confidential information, including but not limited to PII, will be available only to BrightBytes employees and contractors directly supporting the EdTech Impact Solution and Progress Monitoring Platform who have a legitimate educational need to know as determined by the Director of BrightBytes. Prior to the release of District Data, to provide District according to their security guidelines, an email confirmation that each BrightBytes employee and contractor who will have access to confidential information have executed confidentiality terms at least as restrictive as those in the Agreement. Additionally, BrightBytes will adhere to its Privacy Policy (*See* Attachment “F”). Any individual-level student records (e.g., not in aggregate) will be considered confidential information and protected as such, even if student identifiers have been removed from the record.
  2. To utilize District Data provided to BrightBytes only for the purpose of (i) providing the services to the District as contemplated by the Agreement, specifically and exclusively limited to the collection of data from the District as a condition in the District’s participation in the Mississippi Connects Digital Learning Program of the EDLA, and the compiling and provision of the reports set forth in Attachment “D;” (ii) internal purposes of maintaining, supporting, evaluating, improving and developing BrightBytes’ applications and services (including but not limited to, sharing with BrightBytes contractors and consultants for the purposes of research and development related to the Service); and (iii) enforcing BrightBytes’ rights under the Agreement. Use of District Data for any purpose outside the scope of this DSA shall require a written amendment to this DSA or a separate agreement.
  3. Other than to the MDE as contemplated by this Agreement, that no reports created by BrightBytes from District Data will be released in any manner to any individual or any other entity without the prior written consent of the District Superintendent or his/her designee, and that if consent is obtained, only aggregate descriptive statistics will be made available. No report utilizing District data shall be released that will allow the identification of individual students or parents or be easily traceable to a student to whom the information pertains, assuring the use of sufficient cell and subgroup sizes. BrightBytes will only create reports using aggregate descriptive statistics and will use statistical reporting techniques and other measures to prevent the intentional and/or unintentional identification of individuals when producing aggregate reports. BrightBytes will notify the District when any publication is available and provide a copy upon request. BrightBytes shall report all findings directly to the District and share any preliminary and final statistics and/or reports with the District and prior to the release to other entities after approval of the District Superintendent or his/her designee.
  4. That no (i) District Data; (ii) Student Data, or (iii) anonymized, de-identified, or aggregated data created using District Data or Student Data will be sold, transferred, or exchanged by BrightBytes except (i) to MDE as contemplated by this Agreement; or (ii) as expressly permitted by this Agreement.
  5. That any District Data received will be archived in a manner that maintains the confidentiality of the information exchanged and does not permit the identification of individual persons to whom the information pertains. BrightBytes is responsible for the security and confidentiality of District Data in its custody. BrightBytes will use reasonable industry security practices in the storage and use of District Data, as well as student and/or teacher level data. These practices include, but are not limited to:
     1. Restricting physical access to the hardware hosting the data;
     2. Not transmitting PII through unsecured or unencrypted connections;
     3. Limiting access to the system and/or application hosting student/teacher data to only those individuals which have signed a confidentiality agreement, and those vendors or other authorized third-party service providers who have agreed to implement the same security practices;
     4. Physically protecting any backup storage mediums (tape) that contain backups of the data. (i.e., the backups are locked up);
     5. Any cloud-based storage must use Continental United States based data centers;
     6. For any accounts owned or controlled by BrightBytes or its contractors with access to student and/or teacher level data:
        1. Multi-factor authentication;
        2. Non-shared, individual user accounts;
        3. Logging of all access;
        4. Policies and procedures setting access rights and authorizations, including policies that grant access only when absolutely required;
        5. Criminal background checks, to the extent permitted by applicable law, to ensure no such users have any felony convictions, convictions that may indicate a lack of honesty, or are registered sex offenders;
     7. Industry standard physical security and access controls;
     8. Firewalls for all external data connections; and
     9. Implementation of a procedure for regular and timely installation of all necessary software patches and updates.
  6. That in the event the scope of work related to BrightBytes changes or the operations of BrightBytes become compromised due to leadership changes, funding changes, or other factors deemed detrimental by the District, any and all data received in accordance with the provisions in this DSA will be returned to the District upon request with no copies residing with BrightBytes absent the existence of a new written agreement covering the disposition and handling of such data.
  7. If BrightBytes is served with any subpoena, discovery request, court order, or other legal request or command that calls for disclosure of any District Data, BrightBytes shall promptly notify the District in writing and provide the District sufficient time to obtain a court order or take any other action the District deems necessary to prevent disclosure or otherwise protect District Data. Where BrightBytes is prohibited by law from notifying the District of a legal request for District Data, BrightBytes will comply with all applicable laws and regulations with respect to the requested District Data.
  8. To report to District and the MDE within 24 hours of BrightBytes becoming aware of any Data Breach that compromises the security or confidentiality of PII or District Data, unless notification within this time limit would disrupt investigation of the incident by law enforcement. BrightBytes shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the data breach. In the event of a Data Breach related to District Data or PII, BrightBytes agrees to indemnify and hold the District harmless for any loss, cost, damage, or expense suffered by the District as a result thereof. BrightBytes shall also promptly provide the MDE and the District information necessary to enable the District and MDE to fully understand the facts, circumstances, nature and scope of the Data Breach. To the extent the District in its sole discretion deems warranted, the District may provide notice or require BrightBytes to provide notice to any parties, including parents and students, who may have been affected by the Data Breach. In such case, BrightBytes shall consult with the District in a timely fashion regarding appropriate steps required to notify third parties. If the District elects to have BrightBytes provide notice, BrightBytes will pay the entire reasonable cost of such notice, such as mailing, call center services, and, to the extent required by law, identity theft monitoring for affected persons. However, unless otherwise provided by law, in no event will BrightBytes transmit any notice of a Data Breach pursuant to Mississippi Code § 75-24-29 or any other Federal or state law without first obtaining the District’s approval for such notice, which approval will not be unreasonably withheld. BrightBytes shall provide the District and the MDE information about what BrightBytes has done or plans to do to mitigate any deleterious effect or the unauthorized use or disclosure of, or access to, District Data.
  9. At any time during the Term of the Agreement, District may request that BrightBytes retrieve or destroy District Data in BrightBytes’s possession by providing such a request in writing, including but not limited to by the Directive for Disposition of Data (Attachment “G”), which request BrightBytes shall then comply with in a commercially reasonable time not to exceed 30 days. If District requests that BrightBytes retrieve District Data, BrightBytes will provide District with a copy of all District Data that was processed during the Term. For clarity, BrightBytes will continue to maintain a copy of such data for until the end of the Term of the Agreement or until receipt of a destruction request.

# District agrees to:

* 1. Provide only the District Data absolutely necessary for BrightBytes to prepare the reports to MDE set out in Attachment “D,” and District will provide such data to BrightBytes at a mutually agreed upon time after the execution of this DSA by both parties.
  2. Allow BrightBytes to provide mutually agreed upon District Data to the MDE as set out in Attachment “D”, that defines the data, aggregated to the school and district level (no PII), covered by this DSA that will be transferred on the districts’ behalf from BrightBytes to the MDE, attached hereto and incorporated herewith at a mutually agreed upon time after the execution of this DSA by District and BrightBytes.
  3. Allow BrightBytes to access or collect only the Student Data absolutely necessary for BrightBytes to prepare the reports to MDE set out in Attachment “D” and shall facilitate a reasonable method for BrightBytes to access the that limited scope of information stored in District’s student information systems (“**SIS**”), learning management system (“**LMS**”) or other data repository, or receive District Data or other information via SIS, Secure File Transfer Protocol (“**SFTP**”), through the use of the Service or other secure transfer method. To the extent District utilizes a portion of the Service that collects information through a client-layer solution (*e.g.*, a browser extension), network layer solution (*e.g.,* software that resides at the network level and that collects information), or another method that may be used by BrightBytes and/or its third-party service providers to collect information (each a “**Collection Method**”), District authorizes BrightBytes to access or collect District Data and Usage Data (e.g., time spent on page, use of third-party applications, mouse clicks, etc.) via the Collection Method selected by the District in its sole choice or discretion as follows:

\_\_\_\_ Cisco Umbrella; **or**

\_\_\_\_ Chrome extension.

District may, in its sole discretion and without altering or amending this Addendum, change its choice of Collection Method at any time. District agrees that BrightBytes may combine such data with District Data it receives or collects through other methods.

* 1. Make reasonable efforts to work cooperatively with BrightBytes in providing District Data in accordance with the terms of this Agreement. For example: (a) providing a location on a secure server where the data can be safely transferred; (b) creating the data file in an agreed upon format; and (c) providing the data at agreed upon times.
  2. Reserve the right to make unannounced, unscheduled inspections during normal business hours of the District Data utilized by BrightBytes. Such inspections may come in the form of a verbal request to inspect preliminary findings.

**Period of Performance:** The period of performance of the terms and conditions of this DSA shall be from the date of the execution by both parties and will remain in effect until September 30, 2025 (the “Term”) unless terminated earlier or amended under this Agreement.

**Funding:** The parties agree to work cooperatively in the sharing of student data in compliance with FERPA. No funding is involved in the implementation of this DSA.

**COPPA Consent:** The District is under no obligation to obtain written parental consent pursuant to the Children’s Online Privacy Protection Act (“COPPA”), and the District acknowledges that as it pertains to this DSA, the BrightBytes services are utilized for an educational purpose for the use and benefit of the school and for no other commercial purpose.

**Relationship of Parties:** The relationship of District and BrightBytes shall be that of Independent Contractor. None of the provisions of this DSA are intended to create, nor shall they be construed to create an agency, partnership, joint venture, or employer/employee relationship between District and BrightBytes

**Termination:** Either the District or BrightBytes may terminate this DSA at any time by giving ten (10) days written notice to the other party of such termination and specifying the effective date thereof. Furthermore, the District or BrightBytes may terminate this DSA, in whole or in part, upon mutual agreement. Upon termination of this DSA, and at the sole election of the District, BrightBytes will either destroy or return to District all original and copies of District Data regardless of location or deviated form. For clarity and without limitation, BrightBytes is not required to destroy any data that has been aggregated or anonymized, so long as the data is maintained in a form, which could not reasonably be used to identify any individual, taking into account available information.

**Maintenance of Records:** BrightBytes will maintain, as commercially reasonable, pertinent books, documents, and paper or electronic records of BrightBytes solely as related to the charges and performance of BrightBytes under this DSA. Such records shall be kept by BrightBytes for a period of three (3) years from the date of the records, unless the MDE authorizes their earlier disposition. However, if any litigation, claim, negotiation, audit or other action involving the records has been started before the expiration of the three-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it.

**Assignment:** Except as approved otherwise by District in writing,BrightBytes shall not assign or subcontract in whole or in part, its rights or obligations under this DSA without prior written consent of the District and the MDE and all terms and conditions in the DSA apply to both BrightBytes and subcontractors and/or assignments. Any attempted assignment without said consent will be void and of no effect. For the purposes of this DSA, a change of control of BrightBytes shall constitute an assignment requiring prior written consent of both the District and MDE.

**Severability:** Should any term or provision of this DSA be found to be prohibited by the laws of the United States or the State of Mississippi, or should any term or provision be declared invalid or void by a court of competent jurisdiction, the remaining terms, conditions and obligations shall be valid and enforceable to the fullest extent permitted by law, and shall not be affected by the invalidity of any other provision.

**Governmental Entity:** BrightBytes recognizes and acknowledges that the District, as a political subdivision of the State of Mississippi, enters into this DSA only to the extent authorized by Mississippi law, including the opinions of the Attorney General of Mississippi. Any provision that is not authorized by or is inconsistent with Mississippi law, including the opinions of the Mississippi Attorney General, is invalid and deleted.

**Governing Law and Venue:** This DSA is governed and controlled exclusively by the laws of the State of Mississippi. All suits, claims, cases, controversies, actions, disputes, complaints and/or orders related to, arising from, in connection with, or to construe or enforce the DSA shall be governed by the laws of the State of Mississippi, without regard to its conflicts of law principles. The courts of the county in which the District is located shall be the sole and exclusive jurisdiction and venue for any civil action related to this DSA, and BrightBytes irrevocably consents to jurisdiction in said courts and waives any argument that such courts are not a convenient forum for such litigation. Any provision which purports to establish venue outside the State of Mississippi is deleted.

**Indemnification:** Any references to the District indemnifying, defending or holding harmless BrightBytes or any other party are deleted. BrightBytes shall indemnify and hold District and District's affiliates, officers, directors, employees, attorneys and agents harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including attorneys’ fees and costs) arising out of or in connection with: (i) a claim alleging that the services provided by BrightBytes directly infringe a copyright, a U.S. patent, or a trademark of a third party; (ii) a claim, which if true, would constitute a violation by BrightBytes of its representations or warranties, implied or otherwise; or (iii) a claim by any third-party arising from or related to any alleged breach of the DSA by BrightBytes.

**No Limitation of Liability, Remedies, Claims, or Damages:** The District does not agree to limit the liability of BrightBytes in any way. The District does not waive, relinquish, or otherwise limit any remedies, claims, or damages available to it. Any contradictory provisions are deleted.

**Disclaimer of Warranties**: The District does not waive, disclaim or exclude any warranties of any other party to the DSA, including without limitation, such other party’s warranties of merchantability or fitness for a particular use or any common law warranties to which the District is entitled.

**Arbitration:** The District does not agree to submit to arbitration or mediation. Any references to arbitration are deleted.

**No Waiver of Jury Trial or Class Action:** The District does not waive any rights to a trial by jury or to its participation in a class action. Any provisions providing as much are deleted.

**Public Records:** BrightBytes acknowledges that the District and the terms of the Agreement are subject to the Mississippi Public Records Act (“MPRA”), Mississippi Code Annotated §25-61-1 *et seq*. and are not confidential.

**Insurance:** BrightBytes agrees to maintain at all times a cyber liability and data breach policy of insurance providing coverage for expenses, whether incurred by either BrightBytes or the District, in the event of a data breach, privacy incident, digital asset loss, cyber extortion threat, leak, disclosure, or other loss of or damage to the District Data. The limits of such policy of insurance shall be at least Five Million Dollars ($5,000,000.00) per claim or occurrence. Upon request, BrightBytes shall provide proof of such insurance, and advance notification prior to changing insurance carriers.

**Modification or Amendment:** This DSA shall not be modified, altered, or changed, except by mutual, express written consent of the parties. Any modification or amendment shall be made in writing, clearly stating the changes being affected and shall be duly executed by an authorized representative of each party. Any changes of or modifications to the BrightBytes Terms of Service, Privacy Policy, or other things purporting to contractually bind the District or alter this DSA shall be null and void unless such changes are agreed to in accordance with this provision. Any references to BrightBytes’ rights to otherwise modify the terms of the Agreement are deleted.

**Notice:** Any notice required or permitted to be given under this DSA shall be in writing to the party to whom notice should be given at the address set forth below, in addition to the following BrightBytes and District email addresses for legal notifications:

For BrightBytes: legal-notices@google.com

For District: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This Addendum is signed by duly authorized representatives of the parties and is effective as of the date last signed below.

Accepted and agreed to by:

**CUSTOMER**

Signature: Print Name: Print Title: Date:

Accepted and agreed to by:

**BRIGHTBYTES, INC**

Signature: Print Name: Print Title: Date:

District:

NAME

TITLE

ORGANIZATION ADDRESS

BrightBytes:

NAME

TITLE

ADDRESS: 1600 Amphitheatre Parkway, Mountain View, CA 94043

**Entire Agreement:** This DSA with Attachment A, Attachment B, Attachment C, Attachment D, Attachment E, Attachment F, and Attachment G attached hereto and incorporated herein by reference, constitute the entire agreement between the parties with respect to the subject matter contained herein and shall supersede and replace any and all prior negotiations, understandings and agreements, whether written or oral, between the parties hereto.