

CONTRACT BETWEEN
THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY BY AND
THROUGH THE METROPOLITAN BOARD OF PUBLIC EDUCATION
AND
[vendor legal name]
FOR
STUDENT DATA USE AND SECURITY

This Contract is entered into by and between **The Metropolitan Government of Nashville and Davidson County by and through the Metropolitan Board of Public Education** (“MBPE” OR “MNPS”) and **[vendor legal name and address]** (“Recipient”).

By agreeing to these Terms, MBPE authorizes Recipient to access, or receive from MBPE, Student Data and Information (SDI), consisting of Personal Identifiable Information (PII) and/or Confidential Data for the limited purpose of **[brief description of why SDI is collected]**.

In the course of providing Services to MNPS, Recipient will obtain SDI related to students, their families/guardians and MNPS staff. SDI includes but is not limited to:

- All Personally Identifiable Information (“PII”) as defined by the Family Educational Rights and Privacy Act (“FERPA”) (20 U.S.C. §1232g and 34 CFR Part 99), the Children’s Online Privacy Protection Act (“COPPA”) (15 U.S.C. §§6501-6506 and 16 CFR Part 312) and the Individuals with Disabilities Education Act (“IDEA”) (34 CFR Part 300, 20 U.S.C. §1415(a)), and;
- Biometric records, e.g. photos, video, voice recordings and handwriting, as described in FERPA, and;
- All directory data as defined by FERPA, and;
- All education records, as described in FERPA, and;
- All data that are descriptive of or could be used in combination with other data to identify a student or family member / guardian, including, but not limited to, information in the student’s educational record, first and last name, home address, telephone/cell numbers, email address or other information that allows physical or online contact, social security number, student ID number and other identifiers, disciplinary records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, health records, behavioral records, disabilities, socioeconomic information, food purchases, political affiliations, religious information, email, text messages and other network/internet or cellular communications, documents, drawings and artwork, Web search activity, computer/device identifiers and geolocation data, and;
- All data that are derived from, calculated with or linked to SDI by Recipient, and;
- Meta data, e.g. usage logs, Web cookies, Web beacons, records of Web browsing and searches, and;
- All data related to students or their families / guardians that may be provided to Recipient by MNPS or an agent of MNPS, and;
- Any data or metadata that Recipient may collect, calculate or derive based on the use of the Service under this Agreement.

De-identified SDI will have all direct and indirect personal identifiers removed, including any data that could be analyzed and linked to other data to identify the student or family member / guardian. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location data, and school ID. Furthermore, Recipient agrees not to attempt to re-identify de-identified SDI and not to transfer de-identified SDI to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) Recipient gives prior notice to MNPS and MNPS provides prior written consent. Recipient may use de-identified SDI for internal product development and improvement, and research.

In the provision of the Service to MNPS, Recipient is subject to and will comply with applicable laws and regulations, including but not limited to:

- **FERPA:** Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99)
- **IDEA:** Individuals with Disabilities Education Act, (20 U.S.C. § 1400, 34 CFR pt. 300)
- **COPPA:** Children's Online Privacy Protection Act, (15 U.S.C. §§ 6501–6506, 16 CFR Part 312)
- **PPRA:** Protection of Pupil Rights Amendment, (20 U.S. Code § 1232h, 34 CFR Part 98)

SDI linked to students covered by one or more of these laws may be collected, processed and stored within the Services provided by Recipient. The status of individual students may change over time, triggering coverage by a new law and regulation. Recipient agrees to treat all SDI consistently, as covered by and in compliance with all of these laws and regulations.

This Contract is not a Purchase Contract. Execution of this Contract does not in any way obligate MNPS to purchase anything, nor does it imply that MNPS schools or departments are authorized to purchase goods or services from Recipient.

1. **OBLIGATIONS AND ACTIVITIES OF RECIPIENT**

- a. **Permitted Uses of MBPE Student Data and Information (“SDI”).** Recipient shall not use or disclose SDI other than as permitted or required by this Contract or as permitted or required by the Family Educational Rights and Privacy Act (“FERPA”), 34 C.F.R. §99 et. seq and the Children’s Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. § 6501-6506.
- b. **No Marketing or Advertising.** Recipient is prohibited from using SDI to (a) market or advertise to students or families / guardians; (b) inform, influence or enable marketing, advertising or other commercial efforts by a third party; or (c) develop a profile of a student, family member / guardian or group, for any commercial purpose other than providing the Service to MNPS.
- c. **Data Use.** Recipient will use, process and store SDI only for the purpose of providing the Service to MNPS under the Agreement, or to improve the Service delivered to MNPS. Recipient will not use, process or store SDI for other commercial purposes, e.g. marketing, advertising or as part of a product or service offered to a third party.
- d. **Data Analysis and Mining.** Recipient is prohibited from analyzing or mining SDI for any purpose other than delivering the Service to MNPS under this Agreement, or improving the Service for MNPS. Analysis and mining of SDI to support marketing, advertising or other commercial ventures, whether by Recipient or a third party, are prohibited.

- e. **Data Sharing and Re-Disclosure.** MNPS understands that Recipient may rely on one or more sub-contractors to provide the Service under this Agreement, which may have access to SDI. Recipient will provide MNPS with the name and address of each such sub-contractor before this Contract becomes signed and effective. Through the term of the Agreement, Recipient will also provide prior notice to MNPS if Recipient plans to engage a new sub-contractor that may have access to SDI. MNPS may cancel this Agreement if MNPS does not approve of the new sub-contractor.

Recipient is also prohibited from further disclosing any SDI unless re-disclosure is:

- 1) only in furtherance of providing the Service to MNPS, and recipients of re-disclosed SDI agree in writing to comply with the terms of this DSP Amendment and related federal and state laws / regulations that protect SDI, or;
- 2) required to ensure legal and regulatory compliance, or;
- 3) in response to a judicial process in a court in the USA, or;
- 4) to protect the privacy of SDI, the safety of users or others, or the security of the Service.

If any of the four permitted re-disclosure events noted above occurs, Recipient will immediately notify MNPS.

f. **Safeguards.**

- 1) Recipient shall provide MBPE with the name and contact information for a primary and alternate employee of Recipient who shall serve as MBPE's primary security contact and who shall be available to assist MBPE twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a SDI-related Security Breach. The designated contact shall respond to any MBPE inquiries within twenty-four (24) hours.
- 2) SDI will be kept secured in accordance with Section 1.f.3) of this Contract, and the identity of all persons having access to the SDI will be documented and access will be logged.
- 3) Without limiting Recipient's obligations under this Contract to keep SDI safe and confidential, Recipient shall implement administrative, physical, and technical infrastructure and procedural safeguards to protect and maintain the integrity of SDI that Recipient creates, receives, maintains, or transmits on behalf of MBPE. Such safeguards shall be no less rigorous than current industry best practices necessary to secure and protect the confidentiality and integrity of SDI.
- 4) Prior to releasing SDI to any disclosee, Recipient must obtain written agreement from the disclosee that the disclosee will safeguard SDI as required by this Contract.
- 5) MBPE's SDI shall be stored, backed up and served only on US based servers. Third party datacenters used by Recipient for this purpose must be approved by MBPE to serve as Recipient's disclosees.
- 6) Recipient will assure that all data that is transmitted between MBPE's access points and the ultimate server, by Recipient or its disclosees, using current industry best practices.
- 7) Recipient agrees to provide the following additional safeguards:

- a) Include component and system level fault tolerance and redundancy in system design.
- b) Hash user passwords in any data storage location and obfuscate password entry fields in any entry interface controlled by the discloser.
- c) Secure transmission of login credentials.
- d) Provide audit trails and reports of user activity and source IP address.
- e) Secure (encrypt) the audit trails and system generated logs and ensure that they are stored in locations that are inaccessible to automated content discovery software.
- f) Conduct or undergo system level testing whenever new functionalities are added to the system to reconfirm system security measures are retained and functional, and that interaction with MBPE systems is not degraded or compromised.
- g) Employ an in-line Intrusion Protection System that inspects incoming data transmissions.
- h) Ensure that SDI is stored in privately addressed network devices that have no direct interaction with public networks.
- i) Support system security measures testing and verification before receiving, transmitting, or creating SDI.
- j) Maintain a documented Disaster Recovery Plan that includes the following elements:
 - i. Available recovery times.
 - ii. Conduct 24x7 system monitoring that is capable of detecting potential outages.
 - iii. Plans for File-level, Database and server recovery after a component/system failure, damage, or compromise.
 - iv. Substantial geographical separation between data centers hosting production, backup and redundant system elements.
 - v. Include recovery/mitigation procedures for all managed sites, including subcontractors, agents, and other disclosees.
 - vi. Include provisions for at least the following events:
 - 1. Fire
 - 2. Natural disaster
 - 3. Sabotage
 - 4. Accidental human error
 - 5. Flooding
 - 6. Equipment failure
 - 7. Application/database failure
 - 8. Other unlikely events
 - vii. No less than annual testing of the Disaster Recovery Plan (at least parts that affect SDI), with results of the test made available to MBPE, as well as

information about, and schedule for, the correction of deficiencies identified in the test.

- j) Prevention of hostile or unauthorized intrusion.
 - k) Security criminal history screening of employees with access to SDI. Screening is to be conducted by a commercial background screening company, the name of which is to be provided to MBPE. If the criminal history records check indicates that any employee has been convicted in any jurisdiction of a sexual offense, a weapon-related offense, an offense against a child, an assaultive or violent offense, a burglary, a felony offense involving a controlled substance, an identity theft, fraud, or an attempt, conspiracy, or solicitation to commit any of these offenses, Recipient must notify MBPE and put measures in place to ensure that the employee does not have access to the SDI. The security measures put in place to ensure the employee does not have access to the SDI must be approved by MBPE.
 - l) Backup all SDI at least once every 24 hours.
 - m) Perform content snapshots at least daily and retain for at least 90 days.
- g. **Mitigation.** Recipient shall mitigate, to the extent practicable, any actual or potential harmful effect that is known to Recipient of a use or disclosure of SDI by Recipient or Recipient's disclosee in violation of the requirements of this Contract.
- h. **Notice of Disclosure, Security Incident or Breach.**
- 1) In the event that an unauthorized disclosure of SDI, unauthorized access to SDI, or other incident that threatens the security of SDI comes to the attention of Recipient or an Authorized Disclosee, Recipient will immediately take action to close and remediate the breach, determine the scope of the SDI that may have been disclosed, and notify MBPE with the reasons for or cause of the breach, actions taken to close and mitigate the breach, and identification of the SDI that may have been compromised.
 - 2) Immediately following Recipient's notification to MBPE of a security incident, breach, or loss of SDI, the parties shall coordinate with each other to investigate the matter. Recipient shall cooperate with MBPE in investigating the matter and in meeting MBPE's notification obligations under any applicable notification laws. Recipient agrees to fully cooperate with MBPE in MBPE's handling of the matter, including, without limitation:
 - a) Assisting with any investigation;
 - b) Facilitating interviews with Recipient's employees and others involved in the matter;
 - c) Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise required by MBPE;
 - d) Providing the tools and procedures necessary to recapture stored SDI in the event of the loss of such information from the Recipient's and/or disclosee's storage medium.
 - 3) Recipient shall provide the following information to MBPE within five (5) business days of discovery of a security incident, breach, or loss of SDI except when, despite all reasonable efforts by Recipient to obtain the information required, circumstances

beyond the control of the Recipient necessitate additional time. Under such circumstances, Recipient shall notify MBPE, before the five (5) business days have elapsed, of the necessity for additional time. And shall provide to MBPE the following information as soon as possible and without unreasonable delay, but in no event later than fifteen (15) calendar days from the date of discovery of a security incident, breach, or loss of SDI:

- a) The date of the security incident, breach, or loss of SDI;
 - b) The date of the discovery of the security incident, breach, or loss of SDI;
 - c) A description of the types of SDI that were involved;
 - d) identification of each individual whose SDI has been, or is reasonably believed to have been, accessed, acquired, lost, modified, or disclosed; and
 - e) Any other details necessary to complete an assessment of the risk of harm to each individual identified in Section I.d.iii.4) of this Contract.
- 4) Recipient shall provide frequent communications to MNPS on the status of the breach investigation, to be shared with the affected parties, and cooperate with MNPS' efforts to communicate with affected parties by providing MNPS with prior review of all press releases and any communications to be sent to affected parties.
 - 5) Recipient agrees to establish procedures to investigate the security incident, breach, or loss of SDI, to mitigate losses, and to install/implement such safeguards as are needed to protect against any future security incident, breach, or loss of SDI. Recipient agrees to provide a description of these procedures and the specific findings of the investigation to MBPE in the time and manner reasonably requested by MBPE.

2. **COMPLIANCE OF AGENTS**

- a. MBPE may designate third parties who are authorized to securely access its SDI in Recipient's possession/custody. Recipient shall not disclose the SDI to any third party unless MBPE has a current Data Use and Integration Security contract with that third party, Recipient has received prior written approval by MBPE, or such disclosure is required by law.
- b. MBPE may, at any time, revoke any third party or disclosee's access to SDI by providing written notice to the third party or disclosee and Recipient.
- c. Recipient agrees to ensure that any agent, including an Approved Disclosee, to whom it provides SDI created, received, maintained, or transmitted by Recipient on behalf of MBPE, agrees to the same restrictions and conditions that apply through this Contract to Recipient with respect to such information. For all employees or subcontractors who have access to SDI, during the term of each subcontractor or employee's employment by Recipient, Recipient shall at all times cause such subcontractor or employee to abide strictly by Recipient's obligations under this Contract. Recipient further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of SDI by any of Recipient's officers, partners, principals, employees, or agents.

3. **DISCLOSURE OF PRACTICES, BOOKS, AND RECORDS**. Recipient shall make its internal practices, books, and records relating to the access, use, and disclosure of SDI received from MBPE, or SDI created, received, maintained or transmitted by Recipient on behalf of MBPE, available to MBPE or MBPE's designee in a time and manner designated

by MBPE.

4. **INSURANCE.** Recipient shall maintain, throughout the term of this Contract, a stand-alone Cyber/Privacy Insurance policy, naming MNPS as additional insured and loss payee, that provides the coverages shown below. The policy or policies will have combined single coverage of not less than five million dollars (\$5,000,000) per occurrence and five million dollars (\$5,000,000) in the aggregate, except as noted in section 4.a) below.
 - a. **Cyber and Privacy Liability.** Although the preferred coverage for all sub-categories of cyber insurance is \$5,000,000 (five million dollars), the table below can be used as a guide for coverage limits based on the number of MNPS schools in which the Recipient will be providing services.

| Coverage Type | >39 Schools | 25-39 Schools | 10-24 Schools | <10 Schools |
|---|-------------|---------------|---------------|-------------|
| Cyber Liability - Coverage for third party claim arising from hacking or virus | \$5,000,000 | \$3,000,000 | \$2,000,000 | \$1,000,000 |
| Privacy Liability - Coverage for a third party claim arising out of a loss/theft of SDI | \$5,000,000 | \$3,000,000 | \$2,000,000 | \$1,000,000 |
| System Business Interruption | \$2,000,000 | \$500,000 | \$500,000 | \$100,000 |
| Regulatory Actions and Investigations including defense costs and fines/penalties | \$5,000,000 | \$3,000,000 | \$2,000,000 | \$1,000,000 |
| Privacy Breach Notification Costs including Credit Monitoring and costs from an Administrative Breach | \$5,000,000 | \$3,000,000 | \$2,000,000 | \$1,000,000 |
| Cyber Threats and Extortion | \$1,000,000 | \$1,000,000 | \$1,000,000 | \$500,000 |
| Multimedia Liability and Advertising Injury | \$500,000 | \$500,000 | \$500,000 | \$500,000 |
| Crisis Communication Costs | \$2,000,000 | \$2,000,000 | \$1,000,000 | \$500,000 |

Recipient must provide a certificate of insurance, in a form satisfactory to MNPS (e.g. standard ACORD), evidencing such coverages, and provide annual renewal certificates to MNPS throughout the term of this Contract.

Note: If Recipient does not have a stand-alone Cyber/Privacy Insurance policy, MNPS can put Recipient in contact with an insurance broker who specializes in this type of coverage.

5. **INDEMNITY.** Recipient shall indemnify and hold harmless MBPE, its officers, agents and employees from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees, arising out of or in connection with any non-permitted use or disclosure of SDI or other breach of this Contract by Recipient or any subcontractor or agent of the Recipient. To the fullest extent permitted by law, the Recipient shall indemnify and hold harmless MBPE and its employees ("Indemnitees") from and against all claims, liabilities, damages, losses, and costs including, but not limited to, reasonable costs and attorneys' fees at the pre-trial, trial and appellate levels, arising out of, resulting from, or incidental to Recipient's performance under this Contract or to the extent caused by negligence, recklessness, or intentional wrongful conduct of the Recipient, approved disclosees or other persons employed or utilized by the Recipient in the performance of this

Contract. The remedy provided to the Indemnitees by this indemnification shall be in addition to and not in lieu of any other remedy available under the Contract or otherwise. This indemnification obligation shall not be diminished or limited in any way by any insurance maintained pursuant to the Contract otherwise available to the Recipient. The remedy provided to the Indemnitees by this indemnification shall survive this Contract. The provisions of this Section shall specifically survive the termination of this Contract. The provisions of this Section are intended to require the Recipient to furnish the greatest amount of indemnification allowed under Tennessee law. To the extent any indemnification requirement contained in this Agreement is deemed to be in violation of any law, that provision shall be deemed modified so that the Recipient shall be required to furnish the greatest level of indemnification to the Indemnitees as was intended by the parties hereto.

6. **OBLIGATIONS OF MBPE**

- a. MBPE shall notify Recipient of any changes in, or revocation of, permission by MBPE to use or disclose SDI, to the extent that such changes may affect Recipient's use or disclosure of SDI.
- b. MBPE shall notify Recipient of any restriction to the use or disclosure of SDI that MBPE has agreed to, to the extent that such restriction may affect Recipient's use or disclosure of SDI.

7. **TERM, TERMINATION, AND RETURN OF SDI**

- a. **Term.** The Term of this Contract shall be effective as of [effective date] and shall terminate on [termination date – term not to exceed 3 years].
- b. **Termination for Cause.** Upon MBPE's knowledge of a material breach by Recipient, MBPE shall provide an opportunity for Recipient to cure the breach or end the violation. MBPE may terminate this Contract between MBPE and Recipient if Recipient does not cure the breach or end the violation within the time specified by MBPE. In addition, MBPE may immediately terminate this Contract if Recipient has breached a material term of this Contract and cure is not feasible.
- c. **Obligations on Termination.**
 - 1) Except as provided in subsection 2), upon termination of this Contract, for any reason, Recipient shall return or destroy, as determined by MBPE, all SDI received from MBPE, or created or received by Recipient on behalf of MBPE. This provision shall apply to SDI that is in the possession of Authorized Disclosees, subcontractors, or agents of the Recipient. Recipient shall retain no copies of the SDI. Recipient shall complete such return or destruction as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement. Within such sixty (60) day period, Recipient shall certify on oath in writing to MBPE that such return or destruction has been completed.
 - 2) In the event that Recipient determines that returning or destroying the SDI is infeasible, Recipient shall provide to MBPE notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of SDI is infeasible, Recipient shall cease and desist use of SDI except as agreed upon by MBPE. If MBPE does not agree that return or destruction of SDI is infeasible, subparagraph 1) shall apply. Recipient shall complete these obligations as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Contract.

- d. **Rights and License to Confidential Data and Intellectual Property.** The parties agree that:
- 1) All rights to Confidential Data and derivative works created from Confidential Data shall remain the exclusive property of MNPS, and;
 - 2) All rights to MNPS IP shall remain the exclusive property of MNPS and MNPS students and staff, and;
 - 3) Recipient may not sell, trade, rent, lease or otherwise profit from the transfer of Confidential Data or MNPS IP to a third party, and;
 - 4) MNPS grants to Recipient a limited, nonexclusive license to use, process and store the Confidential Data and MNPS IP solely for the purpose of delivering the Service to MNPS under the terms of the Agreement, and;
 - 5) This limited, nonexclusive license granted to Recipient by MNPS expires when the Agreement is terminated.

8. **MISCELLANEOUS**

- a. **Amendment.** This Contract may be modified only by written amendment executed by all parties and their signatories hereto.
- b. **Changes to Policies or Terms of Service**
- 1) Recipient shall not change how SDI are collected, used or shared under the terms of this Contract without advance notice to and prior written consent from MNPS.
 - 2) Recipient shall provide prior notice to MNPS of any proposed change to its terms of service, terms and conditions of use, license agreement and/or privacy policies, at least thirty (30) days prior to the implementation of any such change. MNPS must approve changes in writing, and may terminate the Agreement upon receipt of the prior notice.
- c. **Survival.** The respective rights and obligations of Recipient and MBPE shall survive the termination of this Contract.
- d. **Interpretation.** Any ambiguity in this Contract shall be resolved in favor of a meaning that permits MBPE to comply with FERPA or any applicable regulations in regard to such laws.

9. **EXPORT CONTROL:** Recipient shall not export directly or indirectly any data, information or items acquired under this Contract to any country for which the U.S. Government requires an export license or other approval, without first obtaining such license or approval.

**THE METROPOLITAN GOVERNMENT OF
NASHVILLE AND DAVIDSON COUNTY BY AND
THROUGH THE METROPOLITAN BOARD OF
PUBLIC EDUCATION:**

APPROVED:

Chair, MBPE

RECOMMENDED:

Executive Director of Information Technology, MNPS

Executive Staff Member, MNPS

Director of Purchasing, MNPS

Chief Financial Officer, MNPS

Metropolitan Director of Finance

APPROVED AS TO INSURANCE:

Metropolitan Director of Insurance

APPROVED AS TO FORM AND LEGALITY:

Metropolitan Attorney

**FILED IN THE OFFICE OF THE
METROPOLITAN CLERK:**

Metropolitan Clerk

Date: _____

RECIPIENT:

Signature

Name

Title

Sworn to and subscribed to before me, a
Notary Public, this _____ day of
_____, 20 __, by
_____, the
_____ of the

RECIPIENT and duly authorized to
execute this instrument on Recipient's
behalf.

Notary Public

My Commission Expires _____