

## DATA PROTECTION AGREEMENT

This Data Protection Agreement (“Agreement”) dated as of July 11, 2024 is by and between Forest Park Middle School (“District”) and The Achievement Network, Ltd. (“Contractor”).

In consideration of the mutual covenants, promises, understandings, releases and payments described in this Agreement, the parties agree to the following:

### 1. Definitions

1.1 “*Aggregated District Data*” means an aggregate set of De-Identified Data that does not identify any such data as being related to any specific District students.

1.2 “*District Data*” means any Personally Identifiable Information, Record, Education Record and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of services to the District including all student data inputted into MyANet, Contractor’s technology assessment platform.

1.3 “*De-identified Data*” means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.4 “*Education Records*” means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.5 “*Incident*” means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.6 “*Personally Identifiable Information*” or “*PII*” means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to 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. Personally Identifiable Information includes but is not limited to: (a) the student’s name; (b) the name of the student’s parent or other family members; (c) the address or phone number of the student or student’s family; (d) personal identifiers such as the student’s state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student’s date of birth, place of birth or mother’s maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

1.7 “*Record*” means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.8 “*Securely Destroy*” means to remove District Data from Contractor’s systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology (“NIST”) SP 800-88 r1 (2014) so that District Data is permanently irretrievable in Contractor’s and its Subcontractors’ normal course of business.

1.9 “*Security Breach*” means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Agreement, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.10 “*Services*” means any goods or services acquired by the District from the Contractor, including computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet or installed or run on a computer or electronic device.

1.11 “*Subcontractor*” means Contractor’s employees, subcontractors or agents who Contractor has engaged to enable Contractor to perform services to the District.

1.12 “*Student Profile*” means a collection of PII data elements relating to a student of the District.

## 2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, including without limitation, De-identified Data. The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its services to the District. This Agreement does not give Contractor any rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in this Agreement.

## 3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only as described on Attachment A hereto for the purpose of performing the services and fulfilling its duties to the District.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5 and the permitted uses set forth on Attachment A, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2 Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor’s privacy policy;

3.2.4 Use District Data to create a Student Profile other than as authorized or required by Contractor to perform services for District; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 (“FERPA”), it will be designated as a “school official” with “legitimate educational interests” in the District Education Records and PII disclosed to Contractor in order for Contractor to perform its services to District, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties to the District, and shall not share District Data with or disclose it to any third party except as provided for in this Agreement, as required by law, or if authorized in writing by the District.



3.4 Subcontractor Use of District Data. To the extent necessary to perform its services to the District, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its services to the District; (d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; (e) Subcontractor shall indemnify the District in accordance with the terms set forth in Section 10 hereinbelow; and (f) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees who have potential access to District Data have undergone appropriate background screening, as well as recommending the same to its Subcontractors, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Agreement. Contractor shall also ensure that its Subcontractors comply with the insurance requirements specified in Section 12 of this Agreement.

3.5 Use of De-identified Data. In addition to the permitted uses set forth on Attachment A, Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, the development of new products and services, conduct detailed internal analysis that enables Vendor to analyze performance outcomes and determine how effective its services are and to conduct internal coaching and training for its employees. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

#### **4. Data Security**

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with industry practices, including implementing appropriate administrative, physical, and technical safeguards to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, as well as the terms and conditions of this Agreement.

4.2 Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity.

4.3 Verification of Safeguards. Upon District's written request, Contractor shall provide to the District for review, the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards: (1) a third-party network security audit report, or (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred.

4.4 Background Checks. The Contractor and every person, including any subcontractor or agent of the Contractor, who has unsupervised access to students, or access to student data, shall be required to have a criminal background check. The costs associated with the background check are solely the Contractor's responsibility.

#### **5. Security Incident and Security Breach**

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. Immediately upon becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within ten (10) business days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach.

5.4 Effect of Security Breach. Upon the occurrence of a Security Breach, the District may terminate this Agreement in accordance with District policies. The District may require Contractor to suspend all services, pending the investigation and successful resolution of any Security Breach, and Contractor may be required to reimburse District all amounts paid for any period during which services were not rendered, as provided herein.

5.5 Liability for Security Breach. In addition to any other remedies available to the District under law or equity, Contractor shall reimburse the District in full for all reasonable third party costs, including but not limited to payment of legal fees, audit costs, fines, and other fees imposed that were actually incurred by the District and caused by Contractor or Contractor's Subcontractors for any Security Breach. Contractor shall also provide notification to individuals on behalf of the District, pursuant with Student Data Transparency and Security Act, 22-16-108 (4), whose Personally Identifiable Information was compromised and to regulatory agencies and other entities, and to provide one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during any Security Breach could be used to commit financial identity theft.

## **6. Response to Legal Orders, Demands or Requests for Data**

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall promptly notify the District of any subpoenas, warrants, other legal orders, or demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, the District will promptly notify Contractor and, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3 Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. If another timeline for response is provided herein, then that, more specific, deadline shall control. Otherwise, Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

## **7. Compliance with Applicable Law**

7.1. Children's Online Privacy and Protection Act. In performance of the services to the District, if Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations) from children under thirteen (13) years of age, Contractor



warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with full notice of its collection, use, and disclosure practices.

7.2 Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the services provided to District including but not limited to COPPA and FERPA.

**8. Termination.** This Agreement will become effective when both parties have executed this Agreement ("Effective Date"). This Agreement will automatically terminate with the termination or complete delivery of services by Contractor to the District.

## **9. Data Transfer Upon Termination or Expiration**

9.1 Destruction or Return of District Data. With the exception of (A) De-identified Data that District has agreed to allow Contractor to use after termination or expiration of this Agreement pursuant to Section 3.5, and (B) any District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, within thirty (30) calendar days after termination or expiration of this Agreement, Contractor shall ensure that all District Data and PII that Contractor collected or generated by Contractor is securely returned or Securely Destroyed, as directed by the District. In the event that the District requests destruction, Contractor agrees to Securely Destroy all District Data that is in its possession and cause its Subcontractors to Securely Destroy all District Data that is in the possession of any Subcontractors. If the District requests return, Contractor shall securely return all District Data to the authorized person specified by the District, using the methods requested by the District, in its discretion.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data that is in Contractor's possession or in the possession of Contractor's Subcontractors transferred to a third party designated by the District, such transfer shall occur within a reasonable period of time but no later than thirty (30) calendar days after expiration or termination of this Agreement, and without significant interruption in service or access to such District Data. Contractor shall work closely with such third party transferee to ensure that such transfer/migration uses facilities and methods compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. District will pay all costs associated with such transfer, unless such transfer is as the result of termination of this Agreement following Contractor's breach of the terms of this Agreement. Upon successful transfer of District Data, as confirmed in writing by the District's Designated Representative, Contractor shall Securely Destroy all District Data in accordance with Section 9.1.

9.3 Response to Specific Data Destruction or Return Requests. Contractor shall Securely Destroy or return any specific District Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District.

9.4 Exception to Data Destruction or Return. Notwithstanding the foregoing portions of this Section 9, Contractor shall be permitted to retain and use one copy of De-Identified Data pursuant to Section 3.5.

## **10. Indemnification**

Contractor shall indemnify, defend and hold District and its elected officials, employees, representatives, and agents harmless, without limitation, from and against any and all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses, including reasonable attorneys' fees, the costs of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from Contractor's performance of services under this Agreement, any third-party claim against any Indemnified party arising out of or resulting from Contractor's failure to comply with any of its obligations under

Sections 3, 4, 5, and 9 of this Agreement, and any breach of Contractor’s obligations under this Agreement. These indemnification duties shall survive termination or expiration of this Agreement.

**11. Miscellaneous**

11.1 Survival. The Contractor’s obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

11.2 Governing Law. This Agreement shall be governed and construed in accordance with the laws of Massachusetts, excluding its choice of law rules. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the federal court located in Massachusetts or the state court located in Suffolk County, Massachusetts.

11.3 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District.

11.4 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

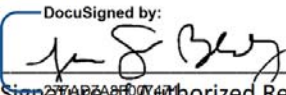
11.5 Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date set forth below each party’s signature.

Forest Park Middle School

THE ACHIEVEMENT NETWORK, LTD.

By:   
Signature of Authorized Representative

DocuSigned by:  
By:   
Signature of Authorized Representative

Jason Stoxen - Technology Manager  
Print Name & Title

Janine Givens-Belsman, Managing Director, Partnerships  
Print Name & Title

Date: 08/01/2024

Date: 7/12/2024

**ATTACHMENT A**

Permitted Use of Student Data.

1.1 Contractor may use Student Data to compile and provide reports containing analysis of student assessment results (the "Reports"), which include: (i) student summaries by whole school, class, grade and student level, (ii) item analysis by grade and (iii) District Network comparisons and out of Network comparisons available through <https://my.achievementnetwork.org>. A "Network" includes all Contractor member schools assigned to District's Network. "District's Network" includes all schools sharing the same Schedule of Assessed Standards as District.

1.2 Contractor and its subcontractors may use De-Identified Student Data to use, compile, distribute aggregated student performance reports ("Aggregated Data Reports") to third parties to which Contractor provides its services.

1.3 Except as otherwise set forth in this Agreement, Contractor shall not disclose or distribute to third parties any District Data other than (a) as part of Aggregated Data Reports, (b) to its subcontractors who require such information in connection with the provision of services to the District, or (c) to third parties for research and evaluation purposes. For clarity, the results of any research described in the foregoing clause (c) may be disclosed, published, distributed and otherwise used by Contractor without restriction, provided that District Data is not revealed in such disclosure, publication, distribution or use other than as part of Aggregated Data. District hereby grants to Contractor and its subcontractors a non-exclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid license to use, reproduce, modify and distribute the District Data in connection with the uses described in the foregoing clauses (a)-(c).