BULLITT COUNTY PUBLIC SCHOOLS

SARAH SMITH, DIRECTOR

DEPARTMENT OF SAFE SCHOOLS

MEMO

To: Dr. Jesse Bacon, Superintendent

From: Sarah Smith, Director of School Safety and Mental Health

Date: Mar 5, 2026

RE: Data Protection for Tier 2 and 3 Character Strong

I am requesting approval of the attached document, the Data Protection Addendum ("Addendum") between the Bullitt County Public Schools and CharacterStrong LLC ("Contractor").

The Addendum outlines essential privacy and security provisions, beginning with definitions for terms such as Personally Identifiable Information (PII), Student Data, and Education Records. It establishes the Contractor as a School Official with a legitimate educational interest. Crucially, the Contractor is strictly prohibited from using BCPS Data for its own commercial benefit, including advertising, and is forbidden from selling, renting, or disclosing the data to any third party without prior consent, except as required by law. Regarding security, the Contractor must implement administrative, physical, and technical safeguards according to commercial best practices, including encrypting electronic data both in transmission and at rest. In the event of a Security Breach, the Contractor is required to notify the BCPS Designated Representative within seventy-two (72) hours. Furthermore, the Contractor warrants compliance with all applicable laws, including FERPA, COPPA, and HIPAA, and must securely destroy or return all BCPS Data within thirty (30) calendar days upon receiving written notice of termination or expiration.

Please consider approving this request; this is crucial to effective Tier 2 and 3 implementation of Character Strong, the district SEL programming that all schools utilize.

cc: Troy Wood, Chief of Operations

1040 HIGHWAY 44 EAST, SHEPHERDSVILLE, KY 40165 (502)869-8000 (502)543-3608 SARAH.SMITH@BULLITT.KYSCHOOLS.US

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is attached to and forms a part of the parties' agreement for services (the "Contract") dated March 23, 2026, by and between Bullitt Co Public Schools ("District") and CharacterStrong LLC ("Contractor") (the Addendum and the Contract are collectively referred to hereinafter as "Agreement"). This Addendum supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect.

In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. "*Biometric Record*," as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.2. "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.3. "*District Data*" means any Student Data, Personally Identifiable Information, Record, Education Records, as defined herein, 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 the Services, as defined herein.

1.4. "*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.

1.5. "*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.

1.6. "*End User*" means individuals authorized by the District to access and use the Services as defined herein.

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

1.8. "*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.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (b) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (c) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (c) 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; and (e) other financial account numbers, access codes, and state- or federal- identification numbers such as driver's license, passport or visa numbers.

1.9. "*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.

1.10. "*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) or as amended Guidelines for Media Sanitization so that District Data is permanently irretrievable in Contractor's and its Subprocessors' normal course of business.

1.11. "*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 Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.12. "*Services*" means any goods or services acquired by the District from the Contractor, or under the contract, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet, installed, or run on a computer or electronic device.

1.13. "*Student Data*" means includes any data, whether gathered by Contractor or provided by District or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute education records for the purposes of this Addendum, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Schedule 5 is confirmed to be collected or processed by the Contractor pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-identified Data, or anonymous usage data regarding a student's use of Contractor's Services.

1.14. "*Subprocessor*" means, for the purposes of this Addendum, an third party Contractor uses for data collection, analytics, storage, or other service to operate and/or improve its Services, and who has access to Student Data.

1.15. "*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

2.1. School Official. The purpose of this Addendum is to describe the duties and responsibilities to protect District Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Contractor shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the District. For the purposes of this Addendum 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 student data including education records; and (3) is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from education records.

2.2. License. Contractor shall be under the direct control and supervision of the District, with respect to its use of 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 obligations specified in the Contract. 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 the Contract.

2.3. Parent Access. To the extent required by law District shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review education records and/or District Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Contractor shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for the District to respond to a parent or student, whichever is sooner) to the District's request for Student 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 Student Data accessed pursuant to the Services, the Contractor shall refer the parent or individual to the District, who will follow the necessary and proper procedures regarding the requested information.

2.4. Separate Account. If student-generated content is stored or maintained by the Contractor, then Contractor shall, at the request of District, transfer, or provide a mechanism for District to transfer, said content to a separate account created by the student.

2.5. Law Enforcement Requests. Should law enforcement or other government entities ("Requesting Party(ies)") contact Contractor with a request for Student Data held by the Contractor pursuant to the Services, the Contractor shall notify District in advance of a compelled

disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the District of the request.

2.6. Subprocessors. Contractor shall enter into written agreements with all Subprocessors performing functions for Contractor in order for Contractor to provide the Services hereunder, whereby the Subprocessors agree to protect District Data in a manner no less stringent than the terms of this Addendum.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

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, 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 the Contract to perform the Services; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative 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 pursuant to the Contract, 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 under the Contract for District's and its End Users' benefit, and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as required by law, or if authorized in writing by the District.

3.4 Subprocessor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subprocessors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a) Subprocessor shall not disclose District Data, in whole or in part, to any other party; (b) Subprocessor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subprocessor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract; (d) at the conclusion of its/their work under its/their subcontract(s) Subprocessor 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; and (e) Subprocessor 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 and Subprocessors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. Additionally, De-Identified Data may be used by Contractor for those purposes allowed under FERPA and the following purposes: (1) assisting District or other governmental agencies in conducting research and other studies; and (2) research and development of Contractor's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Contractor's use of De-Identified Data shall survive termination of this Addendum or any request by District to return or destroy District Data. In no event shall Contractor or Subprocessors 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.

3.6 Privacy Policy Changes. Prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes.

3.7 Advertising Limitations. Contractor is prohibited from using, disclosing, or selling District Data to (a) inform, influence, or enable targeted advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Services to District. This section does not prohibit Contractor from using District Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or District employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using District Data as permitted in this Addendum and its accompanying exhibits.

4. Data Security

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in SANS Top 20 Security Controls, as amended, 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 Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is deidentified in accordance with this Addendum.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, one or more of the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) a third-party network security audit report; (2) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred; (3) district data has been deidentified by Contractor as set forth in the definition of Deidentified Data in section 1.3 of this Addendum.

4.5 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 results of the background check shall comply

with applicable state law and other district requirements, and upon request, be available to the District. The costs associated with the background check are solely the Contractor's responsibility. Before Services begin, each person required to provide a criminal background check shall disclose in writing and sign a notarized affidavit whether or not he or she has been convicted of any charge(s) such as a felony, misdemeanor, or municipal ordinance violation. Thereafter, during the term of the Contract all new personnel, subcontractor(s), third party support personnel and agents, whether paid or not, that are engaged, hired or added to perform the Services, shall be subject to these same requirements before performing Services on Contractor's behalf.

Notwithstanding the criminal background check requirement as set forth above, Contractor hereby warrants that no employee, subcontractor or agent of the Contractor rendering the Services has been convicted of a criminal offense in this or in any other state involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence; and (iii) Contractor shall notify the District immediately upon the discovery or receipt of any information that any person working for the Contractor has been detained or arrested by a law enforcement agency. Contractor understands that allowing any employee, subcontractor, volunteer or agent who is providing Services on Contractor's behalf, access to students, District's records, including PII, or to enter onto the District's property, that has been arrested or convicted of the aforementioned crimes, constitutes a material breach of this Agreement and may result in the immediate termination of this Agreement.

4.6 Duties of District. District shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. District shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted District Data. District shall notify Contractor promptly of any known unauthorized access. District will assist Contractor in any efforts by Contractor to investigate and respond to any unauthorized access.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best 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. Within seventy-two (72) hours of becoming aware of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative 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.

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 seven (7) calendar 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.

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

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, or other legal orders, 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 within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA, the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor shall promptly notify the District and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4 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. 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. 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 ("COPPA")) from children under thirteen (13) years of age in performing the Services, 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 written 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 including but not limited to: (a) COPPA; (b) FERPA; (c) the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) the Health Information Technology for Economic and Clinical Health Act, (e) Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (f) Payment Card Industry Data Security Standards; (g) Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; and (h) Americans with Disabilities Act, and Federal Export Administration Regulations.

7.3 Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will make best efforts to assist the District in providing its Services to End Users pursuant to this Agreement, and will assistance the District in a manner that its system and Services will, at a minimum, conform with all laws, regulations and guidance that apply to accessibility in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973, and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and Services provided or developed by the District including District content.

8. Term and Termination

8.1 Term. This Addendum takes effect immediately as of the Effective Date and remains in full force and effect until the successful completion of the Services, unless earlier terminated under Sections 8.2 or 8.3.

8.2 Mutual Termination. The parties may terminate this Addendum by mutual written consent so long as the Contract has lapsed or has been terminated. Otherwise, subject to Section 8.3, this Addendum will automatically terminate without any further action of the parties upon the termination or expiration of the Contract between the parties or successful completion of the Services. Alternatively, upon re-execution of the Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.3 Termination for Breach. Either party may immediately terminate this Addendum if such party determines, in its sole discretion, that the other party has breached any of the requirements of this Addendum and after such breaching party has received written notice from the non-breaching party regarding the breach and a ten (10) day opportunity to cure.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than (30) calendar days after termination or expiration of this Agreement, and after having received written notice from the District requesting, and specifying its preference for, the return or destruction of the District Data, Contractor shall certify in writing that all District Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data or Contract Data that is in Contractor's possession or in the possession of Contractor's Subprocessors 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. 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. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subprocessors within seven (7) business days, excluding national holidays, after receiving a written request from the District.

10. Miscellaneous

10.1 Survival. 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.

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

10.3 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 -- Designated Representatives
Schedule 2 -- Subprocessors
Schedule 3 -- Written Consent to Maintain De-identified Data
Schedule 4 -- Certification of Destruction/Return of District Data
Schedule 5 -- Schedule of Data

10.4 Counterparts. This Addendum 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.

10.5 THIS ADDENDUM WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE DISTRICT, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE DISTRICT FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS ADDENDUM OR THE TRANSACTIONS CONTEMPLATED HEREBY.

10.6 Effectiveness; Date. This Addendum will become effective when all parties have signed it. The date of this Addendum will be the date this Addendum is signed by the last party to sign it (as indicated by the date associated with the party's signature).

[SIGNATURE PAGE FOLLOWS]

Each party is signing this agreement on the date stated opposite that party's signature.

DISTRICT SUPERINTENDENT

Name_____

Title_____

Date_____

CONTRACTOR NAME

Name_____

Title_____

Date_____

DISTRICT BOARD CHAIRPERSON

Name_____

Title_____

Date_____

OPTION 1

SCHEDULE 1
Designated Representatives

NOTICE REQUIRED	DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Security Breach:		**John Geiselman** **Vice President Cyber Security** **150 Rouse Blvd., STE 210, Philadelphia, PA 19112** **John.Geiselman@FullBloom.org**
FERPA Requests:		**support@characterstrong.com**
Updates to Privacy Policy / Transparency Requirements:		**support@characterstrong.com**
Data Retrieval:		**support@characterstrong.com**
Destruction of Data:		**support@characterstrong.com**

OPTION 2

SCHEDULE 1
Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
	John Geiselman **Vice President Cyber Security** **150 Rouse Blvd., STE 210, Philadelphia, PA 19112** **John.Geiselman@FullBloom.org**

SCHEDULE 2

Subprocessors List

.

Name of Sub-processor	Purpose
Amazon Web Services (AWS)	Hosting (Required)
Clever	Rostering (Required)

SCHEDULE 3
Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	**Purpose for Retention and Use**	**Period of Use**
Student Data	Quality assurance and analytics	Term Of Agreement

I, John Geiselman, as Vice President, Cyber Security and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Representative Name: John Geiselman

Title: Vice President, Cyber Security

Signature: _____

Date: _____

SCHEDULE 4
Certification of Destruction/Return of District Data

I\We, _____, as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on, 20_____ by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subprocessors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subprocessor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on _____, 20___ to _____, by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subprocessors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subprocessor	*Date of Return*	*Return / Transfer Method*

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 5

CharacterStrong Student Data

Data Collected	General Purpose of Data Collected
School Name	Required
Student Name	Required
Student School	Required
School Contact Email	Required
School Contact Name	Required
Student Grade Level	Required
Student ID	Optional
Student DOB	Required
Student Gender	Optional
Ethnicity or Race	Optional
Language	Optional
Student Homeroom	Optional
Teacher/Staff Name	Required
Teacher/Staff Email	Required
Application Use Statistics	Required - Meta data on user interaction with application
Application Technology Meta Data	Required - IP Addresses of users Required - Cookies
Special Indicator	Optional - English language learner information Optional - Specialized education services (IEP or 504)