ARLINGTON CENTRAL SCHOOL DISTRICT

VENDOR DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Supplemental Information about a Master Agreement between
Arlington Central School District and NCS Pearson, Inc.
and
Arlington Central School District Bill of Rights for Data Security and Privacy

1. Purpose

(a) Arlington Central School District (hereinafter "District") and NCS Pearson, Inc. hereinafter "Vendor") are parties to a contract or other written agreement as described in the Supplemental Information about the Master Agreement Exhibit attached hereto pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement").

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between Arlington Central School District and Pearson Education, Inc., that the District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect to the extent of such conflict. In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect to the extent of such conflict.

2. **Definitions**

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b) “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.

(d) “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and the District’s policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4. **Data Security and Privacy Plan**

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor’s Plan for protecting the District’s Protected Data includes, but is not limited to, its agreement to comply with the terms of the District’s Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor’s Data Security and Privacy Plan for protection of the District’s Protected Data throughout the term of the Master Agreement are as follows:

(a) Vendor will implement all applicable state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District’s data security and privacy policy.

(b) Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c) Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between Arlington Central School District and Pearson Assessments." Vendor's obligations described within this section include, but are not limited to:

(i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and

(ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.

(d) Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors) who will have access to Protected Data, prior to their receiving access.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5. **Notification of Breach and Unauthorized Release**

(a) Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to the District by contacting:
Ms. Melissa Erlebacher
Data Privacy Officer
Arlington Central School District
144 Todd Hill Road
LaGrangeville,NY 12540
or via email at merlebacher@acsdny.org

(c) Vendor will cooperate with the District and provide as much information as possible directly to Arlington Central School District Contact or his/her designee about the incident, and such notification shall be in accordance with all legal and regulatory obligations applicable to Vendor in connection with any breach of data privacy or security of the Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Arlington Central School District Contact or his/her designee.

6. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); *i.e.*, they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i) the parent or eligible student has provided prior written consent; or
(ii) the disclosure is required by statute or court order and notice of the disclosure is provided promptly to the District, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so, provided, however, the parties recognize that the use of de-identified data, which contains no personally identifiable information, is needed by the Vendor to provide, evaluate, maintain and improve its services and products. The provisions of this Data Sharing and Confidentiality Agreement shall not be construed to restrict Vendor from maintaining or using de-identified data (including de-identified aggregated data).

(i) To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the District for the reasonable costs of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor.

Parent Bill of Rights for Data Security and Privacy

Arlington Central School District

The Arlington Central School District is committed to protecting the privacy and security of student data, as well as teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

2) Parents have the right to inspect and review the complete contents of their child's education record.

3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4) A complete list of all student data elements collected by New York State is available electronically: Student Data Inventory. A request for the Student Data Inventory can also be made in writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing as follows:

   Ms. Melissa Erlebacher
   Data Privacy Officer
   Arlington Central School District
   144 Todd Hill Road
   LaGrangeville,NY 12540
   or via email at merlebacher@acsdny.org

   or to Privacy Complaint, Chief Privacy Officer
   New York State Education Department
   89 Washington Avenue, Albany, New York 12234
   Complaints may also be submitted using the Report an Improper Disclosure Form.

6) To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7) Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8) Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Arlington Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," (collectively “Protected Data”) as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives Protected Data from the District, the following supplemental information will be included with this Bill of Rights:

1) The exclusive purposes for which the Protected Data will be used by the third-party contractor, as defined in the contract;

   The exclusive purposes for which the Protected Data will be used by the Vendor is for educational purposes in connection with the provision of the Products.

2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

   Vendor employees and subcontractors who have access to the Protected Data receive training for Information Security and Data Privacy Awareness, Information Security Acceptable Use and Code of Conduct.

3) The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

   The duration of the Products varies and is set forth in the Supplemental Information about the Master Agreement attached hereto. Upon expiration of the Master Agreement, the Protected Data will be destroyed. The District may delete the Protected Data at any time using the application interface of the Products. The Vendor can delete Protected Data upon the written request of the account owner.

4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

   A parent, student, eligible student, teacher or principal may challenge the accuracy of Protected Data by providing a written request or notice to the District. Vendor will provide reasonable assistance to the District with any such request or notice.

5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

All Protected Data will be stored in a secured Amazon Web Services RDS database. The security of the Protected Data will be ensured by firewalls, segregated, virtual private clouds for products and environments, separated tiers for servers, data encryption for data at rest (AES 256), role based access and authentication, unique and complex authentication, information security and data privacy training for employees, least use privileges, configuration management, and formal processes for request and approval of accounts.

6) Address how the data will be protected using encryption while in motion and at rest

Protected Data will be protected while at rest by encryption using AES 256. Data in transit is encrypted using TLSv12 and HTTPS.

BY THE VENDOR, NCS Pearson, Inc.

Shantel Love

Name (Print)

Shantel Love (Oct 14, 2020 09:55 CDT)

Signature

Director of Sales Education for Clinical Assessment, a division of NCS Pearson, Inc.

Title

10/14/2020

Date

Supplemental Information about a Master Agreement between

Arlington Central School District and NCS Pearson, Inc. [1]

Arlington Central School District has entered into a Master Agreement with NCS Pearson, Inc., which governs the availability to the District of the following products or services:

Q-global scoring subscriptions for school psychologists and/or speech-language pathologists and/or special education teachers, purchased through Pearson Assessments with Purchase Orders, as follows: one year BASC-3 (#QG1BA3), three year BASC-3 (#QG3BA3 and #QG3BA3NG), five year BASC-3 (#QG5BA3NG), CELF-5 individual score reports (#0150014090), three year CELF-5 (#QG3CF5), one year WAIS-IV (#QG1WA4RW), three year WIAT-III (#QG3WT3CZJ and QG3WT3), five year WIAT-III (#QG5WT5), three year WISC-V (#QG3WC5 and #QG3WC5RW), five year WISC-V (#QG5WC5), one year WPPSI-IV (#QG1WP4RW), three year WPPSI-IV (#QG3WP4RW), three year WRMT (#QG3WR3) (the "Products").

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to

---

[1] Each educational agency, including a school district, is required to publish a "Bill of Rights for Data Security and Privacy" on its website. *See*, Education Law Section 2-d(3)(a) and Part 121.3(a). The Bill of Rights [that is posted on a district's website] must also include "supplemental information" for each contract that the school district enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data [protected by Education Law Section 2-d]. *See*, Education Law Section 2-d(3)(c) and Part 121.3(c).

Nothing in Education Law Section 2-d or Part 121 requires an educational agency to post its third-party contracts on its website *in their entirety*. In addition, nothing in Education Law Section 2-d or Part 121 requires an educational agency to include the "supplemental information" about each contract, within the contract itself.

However, many school districts and other educational agencies have considered it a best practice to include most or all of the required elements of "supplemental information" within each applicable contract, and have complied with the obligation to include the "supplemental information" for each applicable contract with their Bill of Rights, by posting *the text from this page of this Exhibit* from each applicable contract (or a link to this text) on their website in proximity to their Bill of Rights.

comply with all applicable data protection, privacy and security requirements required of Vendor under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreements are Purchase Order #s 2002366 dated 8/08/2019, #2002384 dated 8/08/2019, #2002386 dated 8/08/2019, #2002483 dated 8/12/2019, #2003032 dated 10/01/2019, #2003086 dated 10/07/2019, #2003301 dated 10/29/2019, #2003302 dated 10/29/2019, #184524 dated 6/25/2018, #1901343 dated 7/02/2018, #1901667 dated 7/18/2018, #1901887 dated 7/31/2018, #1902514 dated 9/06/2018, #1902885 dated 10/12/2018, and #1903753 dated 2/13/2019 .
- At any time during the term or upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, the District may delete or otherwise destroy any and all Protected Data using the application interface Q-global products. If requested in writing by the District, Vendor can delete Protected Data and will assist to the extent possible the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon written request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States or Canada. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at

rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.