

ARLINGTON CENTRAL SCHOOL DISTRICT



VENDOR DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Supplemental Information about a Master Agreement between
Arlington Central School District and **Discovery Education Inc.** and
Arlington Central School District Bill of Rights for Data Security and Privacy

1. Purpose

(a) Arlington Central School District (hereinafter "District") and **Discovery Education Inc.** (hereinafter "Vendor") are parties to a contract or other written agreement 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 **Discovery 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. 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.

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 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 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 **Discovery Education Inc.** 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 or assignees) 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, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident,

stop the breach and mitigate any further unauthorized access or release of 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 to the District no later than the time of disclosure, 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.

(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 or its assignees or subcontractors 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 full cost 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 or its subcontractors or assignees.

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," 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 student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 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);
- 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);
- 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;
- 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
- 6) Address how the data will be protected using encryption while in motion and at rest

BY THE VENDOR Discovery Education, Inc

Megan Haller

Name (Print)

Signed by:

D661C3CCF063464...

Signature

EVP - Global Operations

Title

May 20, 2025

Date

Supplemental Information about a Master Agreement between

[Arlington Central School District] and *Discovery Education Inc.*

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

Mystery Science/Discovery Education Inc.

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 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 Agreement commences on [July 1, 2025] and expires on [June 30, 2026]
 - Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist 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 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. 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.

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

As per the Agreement between the undersigned and the School District, this information must be completed by the Service Provider within ten (10) days of execution of the Agreement.

Name of Provider:	Discovery Education, Inc
Description of the purpose(s) for which Provider will receive/access PII:	To provide contracted services
Type of PII that Provider will receive/access:	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term:	Contract Start Date: <u>TBD</u> Contract End Date: _____
Subcontractor Written Agreement Requirement:	Provider will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by State and Federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Provider will not utilize subcontractors. <input checked="" type="checkbox"/> Provider will utilize subcontractors.
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Provider shall: <ul style="list-style-type: none"> Securely delete and destroy data.
Challenges to Data Accuracy:	Parents, teachers, or principals who seek to challenge the accuracy of PII will do so by contacting the School District. If a correction to data is deemed necessary, the School District will notify Provider. Provider agrees to facilitate such corrections within 21 days of receiving the School District's written request.

Secure Storage and Data Security:	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution.</p> <p><input type="checkbox"/> Other:</p> <p>Amazon Web Services, United States</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Discovery Education maintains ISO 27001 And SOC 2 Type 2 certification. We implement appropriate technical and organizational security measures, such as access controls and encryption, to protect the personal information that we collect and maintain from unauthorized access.</p>
Encryption:	Data will be encrypted while in motion and at rest.

PROVIDER'S DATA PRIVACY AND SECURITY PLAN

Provider must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the School District's website, Provider should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

Name of Provider: Discovery Education, Inc

Address: 4350 Congress St, Suite 700, Charlotte, NC 28209

Email/Phone: decommercialopsteam@discoveryed.com

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	The Contractor Customer and Technical Support team is available to work with District administrators and teachers. There are no fees associated with customer and technical support services. Contractor's support structure includes a defined internal escalation path utilizing a ticket system, which allows a customer to track progress working with any
2	Specify the administrative, operational, and technical safeguards and practices that you have in place to protect PII.	The Contractor Customer and Technical Support team is available to work with District administrators and teachers. There are no fees associated with customer and technical support services. Contractor's support structure includes a defined internal escalation path utilizing a ticket system, which allows a customer to track progress working with any
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the Federal and State laws that govern the confidentiality of PII.	The Contractor will ensure that its personnel and subcontractors that access the student data are informed of the confidential nature of the student data and are bound by appropriate obligations of confidentiality or are under an appropriate statutory obligation of confidentiality. The Contractor will take all reasonable steps and to ensure the reliability of Vendor's personnel and subcontractors that
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	The Contractor employees and any subcontractors are bound by the Discovery Education's Data Privacy found here: https://www.discoveryeducation.com/data-%20protection-addendum/
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the School District.	If District/customer/distributor or Contractor determines that a breach has occurred, when there is a reasonable risk of identity theft or other harm, or where otherwise required by law, Contractor provides any legally required notification to affected parties as promptly as possible, and fully cooperates as needed to ensure compliance with all breach of confidentiality laws. Contractor reports as promptly as possible to District/customers/distributors (or their designees) and
6	Describe how data will be transitioned to the School District when no longer needed by you to meet your contractual obligations, if applicable.	Upon termination or expiration of the contract, the Vendor will destroy/delete student data.

7	Describe your secure destruction practices and how certification will be provided to the School District.	Upon termination or expiration of the contract, the Contractor will destroy/delete student data using a NIST 800-88 compliant method. Upon request, Contractor shall provide certification of data destruction.
8	Outline how your data security and privacy program/ practices align with the School District's applicable policies.	The comprehensive Contractor's Data Privacy can be found here: https://www.discoveryeducation.com/data-%20protection-addendum/