

West Seneca, NY 14224

5/1/2024  
Date: \_\_\_\_\_

## EXHIBIT D

### Data Sharing and Confidentiality Agreement

INCLUDING  
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY  
AND  
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

#### 1. Purpose

- (a) This Exhibit supplements the Master License and Service Agreement (“MLSA”) to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES’ website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

#### 2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.
- (d) “Participating Educational Agency” means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor’s Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor’s Product pursuant to the MLSA to support its own educational programs or operations.

### 3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of all Protected Data it receives in accordance with applicable federal and state law (including but not limited to Section 2-d) and this DSC Agreement, as may be amended by the Parties, and Erie 1 BOCES’ policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and that Erie 1 BOCES will provide Vendor with a copy of its policy upon request.

### 4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES’ Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

#### Typesy Privacy

##### I. Overview

eReflect Software is strongly committed to protecting the privacy of its Clients and of its interactive products and services. Throughout cyberspace, we want to contribute to providing a safe and secure environment for all our Clients, Customers and Visitors. This privacy policy applies to the Typesy (a product of eReflect Software) site and all of the other Internet-accessible Typesy-branded services, which we will from this point forward refer to as Typesy to make reading this policy easier. The purpose of this Typesy privacy policy is to inform you, as a Client of Typesy, what kind of information we may gather about you, how we may use that information, whether we disclose it to anyone, and the choices you have regarding our use of and your ability to correct the information.

Typesy offers a version made available through schools that will be referred to as Typesy EDU and a number of other versions which will be collectively referred to as Typesy Individual. The personal information that we collect, use, share and disclose will depend on which version of Typesy you use.

Most of Typesy is a general audience website. We do not knowingly collect information from children located in the United States under the age of 13 and children located in the European Union under the age of 16. However, some parts of Typesy including but not limited to Typesy EDU are designed for students who may be children. Students may access the sections of Typesy directed at children only after their teacher or school official has entered into an agreement with Typesy.

Finally, please note that this policy applies only to Typesy and Web sites that carry the Typesy brand. This policy does not apply to other eReflect Software websites or apps, or companies or organisations' websites to which we link. We have clearly marked the Typesy site and these branded Web sites with our logo so you know where this policy applies.

## II. Definitions

“Client”: The trader being a company, partnership, sole trader or other organisation or any individual, which undertakes to accept Typesy Services.

“Partner”, “Affiliate”: A third-party organisation that provides Internet development, hosting and/or Internet access services and/or other services to Typesy and/or Client.

“Services”, “Products”: Computer software, upgrades, technical support, ordering information, order processing, help desk communication, emails, newsletters, or any other product, service, and/or means of communication solicited by and provided to Typesy Clients, Partners, and/or Affiliates.

## III. Collecting Information

About All Typesy Software Web Site Visitors: In general, our service automatically gathers certain usage information like the number and frequency of visitors to Typesy, like television ratings that tell the networks how many people tuned in to a program. We only use such data in the aggregate. This collective data helps us determine how much our Clients use parts of the site, so we can improve our site to assure

that it is as appealing as possible. For example, Typesy uses “cookies,” a technology that tells us how and when pages in the site are visited, and by how many people. Typesy cookies do not collect personally identifiable information and we do not combine information collected through cookies with other personally identifiable information to tell us who you are or what your screen name or email address is. We also may provide statistical “ratings” information, never information about you personally, to our Typesy partners about how our members, collectively, use Typesy. We do this so they can understand how many people use our site in order for them to provide you with the best possible experience. The following are ways that our service automatically gathers information about usage:

1. “Cookies”: A cookie is a piece of data stored on the user’s hard drive containing information about the user. Cookies are in no way linked to any personally identifiable information on our site. Once the Client closes their browser, the cookie terminates. For example, if a Client sets a cookie on the site, the Client would not have to enter a password more than once. If a Client rejects the cookie, they may still use the site, but the Client will be limited in some areas of the site.

2. Log Files: We use IP addresses to analyse trends, administer the site, track Client movement, and gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

3. “Tell-A-Friend”: If a Client elects to use our referral service for informing a friend about our site, we ask the Client for the friend’s name and email address. Typesy will automatically send the friend a one-time email inviting them to visit the site. Typesy stores this information for the sole purpose of sending this one-time email. The friend may contact Typesy to request the removal of this information from our database.

#### IV. Collecting Personal or any Specific Information via On-Line Forms

Sometimes, we may specifically ask for information about you (for example, when you request technical support, or when you order a product). We may need certain information, such as name, email address, billing address, type of computer or credit card number in order to provide that service or product. We may also use that information to let you know of additional products and services that might interest you. You can choose not to receive such information by letting us know on the registration screen when you sign up for the product or service. We may ask you for information about your interests so that both you and Typesy can take advantage of the interactivity of the online medium, but you may always choose to respond or not. Additionally, we may provide you with an opportunity to be listed in a directory on one of our Typesy Branded services; these listings are also optional and you can make changes to or eliminate

this information when you want to. The following are ways we may collect personal or specific information:

1. “Registration”: In order to use some parts of the Typesy Website or gain information about a certain product and/or services, the Client must first complete the registration form. During registration the Client is required to give their contact information (such as name and email address). This information is used to contact the user about the services on our site about which they have expressed interest.

2. “On-Line Payment”, “Shopping Cart”: We request information from the Client on our order form and/or service payment form. Here the Client must provide contact information (such as name and shipping address) and financial information (like credit card number, expiration date). This information is used for billing purposes and to fill the Client’s orders. If we have trouble processing an order, this contact information is used to get in touch with the Client. We share this information with Braintree, payment processing software, to process payments from our users.

3. “Surveys and Contests”: From time to time Typesy requests information from users via surveys or contests. Participation in these surveys or contests is voluntary and the Client therefore has a choice whether or not to disclose this information. Information requested may include contact information (such as name and shipping address), and demographic information (such as zip code or age level). Contact information will be used to notify the winners and award prizes. Survey information will be used for purposes of monitoring or improving the use and satisfaction of the relevant Typesy Site, Service or Product.

4. “Newsletters and Notifications”: If the Client wishes to subscribe to our newsletter(s) or notifications (Special Offer, Site, Product and Service Updates, etc.) – we ask for contact information such as the Client’s name and email address. The Client will always be able to unsubscribe from such newsletters and/or notifications by using the unsubscribe links located in the emails or by contacting [helpdesk@erelect.com](mailto:helpdesk@erelect.com).

If you have an account with Typesy we will still send you non-promotional communications, such as service-related emails.

## V. Children’s Information

Children under the age of 13 in the United States and children under the age of 16 in the European Union are not permitted to create their own account on Typesy without the consent of a parent or legal guardian. If you are the parent or legal guardian of a child who has provided us with personal information without your consent, please contact [helpdesk@ereffect.com](mailto:helpdesk@ereffect.com) so we can delete such information.

Children may use Typesy EDU provided the school has complied with its responsibilities under the Family Educational Rights and Privacy Act ("FERPA") and Children's Online Privacy Protection Act ("COPPA").

If a teacher or school official has consented to our collection of information from children who are students in a manner consistent with COPPA, we will collect and use such personal information solely for the use and benefit of the school and for no other commercial purpose. As such we do not send promotional material or surveys to children using Typesy EDU. A school or district must obtain the consent of a parent or legal guardian before providing Typesy with any child's personal information. A parent or school official may revoke at any time their consent to allow children to use Typesy EDU.

#### VI. Parent's Rights

Upon request from a parent or legal guardian, we will provide a description of the personal information we collect, give parents the opportunity to review their child's personal information or have their child's personal information deleted. Such requests can be made by contacting [helpdesk@ereffect.com](mailto:helpdesk@ereffect.com).

#### VII. Use, Collection and Retention of Client Information

Typesy collects, retains and uses only the information about our Clients that is required by law to administer Typesy business and provide high-level services to our Clients. We retain this information no longer than necessary to meet these objectives.

#### VIII. Maintenance of Accurate Information

Typesy has established procedures so that a Client's financial and personally identifiable information is accurate, current and complete in accordance with reasonable commercial standards. Any request to correct inaccurate information is responded to in a timely manner.



#### IX. Limiting Employee Access to Information

All Typesy employees are educated about the importance of privacy and confidentiality. Only those employees having a business reason for knowing such information have access to personally identifiable information.

#### X. Protection of Information via Established Security Procedures

Typesy maintains rigorous security standards and procedures regarding unauthorised access to Client information. Therefore we do not intend to send or receive any sensitive information (such as passwords or credit card information) in an unprotected way or via unencrypted emails.

#### XI. Maintaining Client Privacy in Business Relationships with Third Parties

We do not use or disclose information about your individual visits to Typesy Sites or information that you may give us, such as your name, address, email address or telephone number, to any outside companies. But sometimes it is necessary to provide personally identifiable Client information to a third party. If so, Typesy shall insist that the third party adheres to similar privacy principles that are provided for keeping such information confidential and Client authorisation should be requested.

#### XII. Restrictions on the Disclosure of Account Information

Typesy provides information about Client's accounts or other personally identifiable data to third parties only when: (1) the information is provided to help complete a Client-initiated transaction; (2) the Client requires it; (3) the disclosure is required by or allowed by law; or (4) it is necessary to process transactions and provide our services.

#### XIII. Disclosure of Privacy Principles to Clients

Typesy Clients have the right to know what information we keep about them and how the information is used. Clients have the right to have any inaccurate information corrected or deleted. You can submit a request to review, update or delete any personal information that eReflect stores about you by emailing [helpdesk@ereffect.com](mailto:helpdesk@ereffect.com)

#### XIV. Unsolicited E-mail Circulars Policy

Unsolicited email circulars (SPAM) are becoming an increasing nuisance to Internet users. These mass direct mail-shots can cause inconvenience, annoyance and expense to recipients. Typesy does not condone such practices in any form, nor do we sanction such applications by other websites.

#### XV. International Data Transfers

Typesy and its services operate on servers located in the United States. By using Typesy you consent to the collection, transfer, processing and storage of your information in the United States.

#### XVI. Typesy Privacy Policy Changes

If we decide to change our privacy policy for Typesy, we will post changes here so that you will always know what information we gather, how we might use that information, and whether we will disclose it to anyone. If making any material changes that increase our rights to use of personal information we will obtain consent through an email or posting on our sites.

#### XVII. Summary

All services provided by Typesy to the Client are subject to the above Typesy Global Privacy Policy.

#### XVII. Contact Information

If you have any questions or concerns about this policy, you can contact Typesy by emailing us at [helpdesk@ereflect.com](mailto:helpdesk@ereflect.com) or by writing to us at 3651 Lindell Rd. Suite D1104, Las Vegas, NV 89103.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.



- (b) As required by the NIST Cybersecurity Framework, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA,
  - a. Vendor will have the following reasonable administrative, technical, operational, and physical safeguards and practices in place throughout the term of the MLSA:
    - i. Data Security:
      - 1. Data-at-rest & data-in-transit is encrypted
      - 2. Data leak protections are implemented
    - ii. Information Protection Processes and Procedures:
      - 1. Data destruction is performed according to contract and agreements
      - 2. A plan for vulnerability management is developed and implemented
    - iii. Protective Technology:
      - 1. Log/audit records are ascertained, implemented, documented, and reviewed according to policy
      - 2. Network communications are protected
    - iv. Identity Management, Authentication and Access Control:
      - 1. Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized dev
- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor [check one] \_\_\_\_\_ will X will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, 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 Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 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 state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are 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.

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

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data 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 Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at [mokal@e1b.org](mailto:mokal@e1b.org), or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or 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 personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies 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, Erie 1 BOCES, 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 shall not provide this notification to the CPO directly. 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 Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.


**EXHIBIT D (CONTINUED)****ERIE 1 BOCES****PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 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 to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

**BY THE VENDOR:**

DocuSigned by:

 **Signature**  
74873B5624C3410...**Matthew D. Strine****Printed Name****Sales Director, Northeast****Title**

5/1/2024

**Date**

**EXHIBIT D (CONTINUED)**

## SUPPLEMENTAL INFORMATION

## ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT

## BETWEEN

ERIE 1 BOCES AND *eReflect, Inc.*

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with *eReflect, Inc.* which governs the availability to Participating Educational Agencies of the following Product(s):

*Typesy*

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with *eReflect, Inc.* which governs the availability to Participating Educational Agencies of the following Product(s):

*Typesy*

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

**Exclusive Purpose for which Protected Data will be Used:** The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: *We have limited such third-party providers to Amazon AWS and Microsoft Azure. These providers are required to comply with strict privacy standards and will abide by the provisions of all privacy and security agreements.*

**Duration of MLSA and Protected Data Upon Expiration:**

The MLSA commences on May 1, 2024 and expires on June 30, 2027.

Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

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 Erie 1 BOCES 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 Erie 1 BOCES 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 a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

**Data Storage and Security Protections:** Any Protected Data 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 will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

**Encryption of Protected Data:** Vendor (or, 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 specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.