Idaho Literacy Tools Approved Vendor List
Effectiveness Review Guidance

Per Idaho Code 33-1807, vendors who operate "adaptive learning technology literacy intervention tools" that are computer-based and used for interventions for student in kindergarten through third grade may apply to be on the Literacy Tools Approved Vendor List. Once on the Approved Vendor List for a school year, vendors are required to participate in an annual Effectiveness Review to determine if the vendor and program may remain on the Approved Vendor List. This document provides guidance for Approved Vendors regarding the Effectiveness Review process.

I. DEFINITIONS

"Aggregate Data" means data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that shall encode data to protect its confidentiality.

"Data Storage" refers to the location and/or medium where data are permanently or temporarily reside. Data shall be stored on secured environments.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

"Disclosure" means to permit access to or release, transfer, or other communication of PII contained in education or employment records by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record (34 CFR 99.3).

"Personally Identifiable Information" or **"PII"** means information that can be used to distinguish or trace an individual's identity, such as the student's name, the name of the student's parent or other family, a personal identifier such as the student's social security number, student education ID, biometric records date and place of birth, mother's maiden name, which alone or when combined with other personal or identifying information may be linked or linkable to a specific individual. PII also includes other information that alone or in combination would 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.

I. DATA SECURITY REQUIREMENTS

All data storage and transmission shall be done in compliance with Idaho Code 33-133 and in alignment with the policies and practices established by the Idaho Data Management Council.

DATA TRANSMISSION

To ensure PII Data are encrypted during data transmission, all data including PII shall be electronically transmitted to / from the VENDOR using secure methods.

1) OSBE will provide a secure system for the VENDOR to submit PII Data to OSBE.
2) The VENDOR is required to provide a secure process for client districts and/or schools to submit PII Data to the VENDOR. The secure system / process for PII transmission must ensure PII Data is encrypted in transit or at rest.
    - VENDOR will not receive or transmit PII Data via e-mail.
    - VENDOR will not receive or transmit PII Data via Google Drive or a similar non-secure web sharing system.

DATA STORAGE

All PII Data provided by districts and/or schools to the VENDOR shall be stored by the VENDOR on a secure, encrypted environment with access limited to the least number of staff needed. See Appendix A for additional details.

BREACH OF DATA SECURITY

If VENDOR detects a compromise or potential compromise in the IT security for Data such that PII may have been accessed or disclosed without proper authorization, VENDOR shall give notice to OSBE within one (1) business day of discovering the compromise or potential compromise. VENDOR shall take corrective action as soon as practicable to eliminate the cause of the breach and shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed and take all steps necessary to protect against the improper use of any disclosed PII Data. Vendor shall take full responsibility for the security of all PII Data in its possession, and shall indemnify and hold OSBE harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof.

DATA CONFIDENTIALITY

VENDOR acknowledges the personal or confidential nature of PII Data and agrees to comply with all laws, regulations, and policies that apply to protection of the confidentiality of the data. PII Data gathered for the purpose of the Effectiveness Review shall not be shared with any other entities besides OSBSE unless written authorization is given by OSBE.

II. REQUIRED DELIVERABLES

1. Student Roster, to include all Idaho K-3 students who used the vendor's approved program for the identified school year
2. Vendor Data Analysis, providing aggregate data from the vendor's approved program, demonstrating Idaho students' performance for the identified school year

III. STUDENT ROSTER REQUIREMENTS AND RECOMMENDATIONS

Approved Vendors may not add or delete any columns from the provided template without prior permission from the OSBE Program Manager who is supporting the project.

Approved Vendors must follow all Data Security procedures (outlined above) when gathering and transmitting student personally identifiable information (PII) to or from OSBE, Idaho school districts and/or Idaho schools.

Required fields:

- Idaho District ID #, as aligned to the list provided by the Office of the State Board of Education (OSBE) in the template
- Idaho School ID #, as aligned to the list provided by OSBE in the template
- Student First Name
- Student Last Name
- Student Grade, as enrolled during the identified school year
- Student Met Vendor Usage Threshold, as defined by the vendor
- Total Minutes Student Usage (in the vendor's approved program)

Strongly Recommended fields:

- EDU ID, the 9 digit number assigned by the state to identify the student

IV. VENDOR DATA ANALYSIS REQUIREMENTS AND RECOMMENDATIONS

Vendors are required to conduct an internal analysis of their own data for Idaho students. Vendors' Data Analysis report not be less than 4 pages or exceed 12 pages (typically 4-8 pages is adequate). Previous vendor analyses are summarized in our FY 22 and FY 23 Effectiveness Review reports, as posted on the OSBE website. If you have additional questions, please reach out.

Required in the vendor's analysis:

- Data on the performance of Idaho students in kindergarten through third grade who used the vendor's approved program. Vendors may focus their analysis on all Idaho K-3 students who used the product, all Idaho K-3 students who met the vendor's usage threshold, or both. If any data is included for students who met the vendor's usage threshold, this threshold must be clearly defined.
- Data that reflects student-level growth data (% of students that made growth while using your program and amount of growth seen).
- Data that reflects overall end-year performance of Idaho students in the vendor's approved program.
- Some figures, graphs, or tables representing Idaho students' performance, particularly a graphical representation of Idaho K-3 students' fall to spring growth.

Provided that vendors include all of the above in their analysis, vendors may present their data as appropriate for their specific product.

Recommended for inclusion in the vendor's analysis:

- If the vendor has data that allows for a comparison between their Idaho data and national norms or performance of students who used the approved program in other states, we encourage the vendor to include that.

Optional aspects of the vendor's analysis:

- The vendor's analysis may include data for grades above K-3. If a vendor chooses to provide data for other grades, the vendor must present the K-3 data separately. The vendor may either do analyses on ALL students and K-3 students separately or K-3 students and 4+ students separately, as appropriate based on the product and n sizes.
- A vendor may include additional analyses as they believe appropriate, provided that the requirements listed above are met. If a vendor has questions regarding whether an analysis is appropriate for inclusion, the vendor should contact the OSBE manager and/or contractor supporting the project.

V. HOW VENDORS CAN IMPROVE THEIR STUDENT ROSTER MATCH RATES

- ✓ Get as many student EDU IDs as possible. EDU IDs are a 9-digit number issued by the state. District and/or school IDs are not helpful for the matching process.
- ✓ If possible, require or request that EDU IDs be submitted in your program system during student onboarding, either as the primary student identifier or as supplemental information.
- ✓ If you are not able to gather student EDU IDs during onboarding (particularly for prior years of data), reach out to districts and schools during the school year, well before your student roster is due, and give them plenty of time to submit EDU IDs. **Ensure that you follow all Data Security Requirements (as outlined above and in Appendix A) when transmitting or storing data from Idaho districts or schools.**
- ✓ Ensure that the Student Grade field accurately represents the grades in which students were enrolled for the identified year.

Sample language for Idaho district and school communications and/or contracts

The following sample language is designed to support Vendors in requesting that Idaho districts and/or schools provide student EDU IDs (either through their onboarding or after the school year has completed):

> [Vendor Name] is on the Literacy Tools Approved Vendor List, as established by Idaho Code 33-1807, and overseen by the Idaho Office of the State Board of Education (OSBE). Per statute, [Vendor Name] must participate in an annual Effectiveness Review to remain on the Approved Vendor List. To conduct this review OSBE requires vendors to submit a student roster including all students in Idaho who used [Vendor Name]'s approved program during a given school year.

In order for OSBE to ensure completion of the Effectiveness Review, student EDU IDs are needed to match students to the existing data (student performance, demographics, etc.) that is stored in the state's data system.

To ensure that the students' personally identifiable information (PII) is protected, we require our client districts and schools to provide student EDU IDs through [describe appropriate onboarding process and/or name of specific secure server]. We have confirmed that this system meets the data security requirements outlined by OSBE. Please note that PII Data should never be transmitted by e-mail, Google Drive, or a similarly non-secure system.

If you have questions about our process for data transmission, storage, or security, please contact [Vendor contact]. If you have questions about [Vendor Name]'s status on the Literacy Tools Approved Vendor List or OSBE's oversight of the annual Effectiveness Review Process, please contact Alison Henken at alison.henken@osbe.idaho.gov.

APPENDIX A: Additional Data Storage Expectations

Protection of PII Data

VENDOR will store and protect PII Data only on one or more of the following media:

1) Workstation Hard disk drives. Access to the PII Data stored on local work station hard disks shall be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. If the workstation is located in an unsecured physical location, the hard drive shall be encrypted to protect PII Data in the event the device is stolen.

2) Network server disks. Access to PII Data stored on hard disks mounted on network servers and made available through shared folders shall be restricted to authorized users through the use of access control lists. Access shall be granted only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanism that provides equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers shall be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Backup copies for Disaster Recovery purposes shall be encrypted if recorded to removable media.

3) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. PII Data provided by SBOE on optical discs shall be used in local workstation optical disc drives and shall not be transported out of a secure area. When not in use for the Agreement purpose, such discs shall be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access PII Data on optical discs shall be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

4) Optical discs (e.g. CDs, DVDs, Blu-Rays) in drives or jukeboxes attached to servers. PII Data provided by SBOE on encrypted optical discs shall be attached to network servers and that shall not be transported out of a secure area. Access to PII Data on these discs shall be restricted to authorized users through the use of access control lists that shall grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms that provide equal or greater security, such as biometrics or smart cards. PII Data on optical discs attached to such servers shall be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

5) Paper documents. Any paper PII Data records shall be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records shall be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

6) PII Data storage prohibited outside of the United States. In the event the Agreement requires VENDOR to store, process or transfer PII Data, VENDOR shall store, process, and transfer PII Data only in or to facilities located within the United States.

7) PII Data storage on portable devices or media.

   a) PII Data shall not be stored by VENDOR on portable devices or media unless specifically authorized in writing by SBOE. If so authorized, the PII Data shall be given the following protections:

      i. Encrypt PII Data with a key length of at least 128 bits

      ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.

      iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

      iv. Physically protect the portable device(s) and/or media by:

         - Keeping them in locked storage when not in use;
         - Using check-in/check-out procedures when they are shared; and
         - Taking frequent inventories.

   b) When transported outside of a secure area, portable devices and media with PII Data shall be under the physical control of VENDOR staff with authorization to access PII Data.

   c) Portable devices include, but are not limited to; handhelds/PDAs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.

   d) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs, Blu-Rays), magnetic media (e.g. tape, or Zip disks), or flash media (e.g. CompactFlash, SD, MMC).

Safeguards Against Unauthorized Access and Re-disclosure

VENDOR shall exercise due care to protect all PII Data from unauthorized physical and electronic access. VENDOR shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information:

1) Access to the PII Data shall be restricted to those authorized staff, officials, and agents who need it to perform their official duties in the performance of the work requiring access to PII Data as detailed in this Agreement.

2) VENDOR shall store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.

3) VENDOR shall not store any PII Data on portable electronic devices or media, including, but not limited to laptops, handhelds/PDAs, Ultramobile PCs, flash memory devices, floppy discs, optical discs (CDs/DVDs), and portable hard disks.

4) VENDOR shall protect PII Data in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

5) VENDOR shall take precautions to ensure that only authorized personnel and agents are given access to PII Data.

6) VENDOR shall instruct all individuals with access to PII Data regarding the confidential nature of the information, the requirements of Use of Data and Safeguards against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of PII Data covered by this Agreement.

7) VENDOR shall take due care and take reasonable precautions to protect PII Data from unauthorized physical or electronic access. VENDOR shall meet or exceed the requirements of the Idaho Data Management Council's policies and standards, accessible at: https://boardofed.idaho.gov/research_stats/data_managment_council.asp, for data security and access controls to ensure the confidentiality, availability, and integrity of all PII Data accessed.