3rd Party Vetting & Contract Management

Safety 360 Seminar

July 10, 2024

3rd Party Vetting & Contract Management

- Does your district use educational, operational and administrative software, web-based tools & solutions or mobile applications in your district ?
- Do you know every software, web-based tools & solution or mobile applications that your staff are using?
- Do you know what private information is getting put in every software, web-based tools & solution or mobile applications?

3rd Party Vetting & Contract Management

- **Why do we need to vet 3rd Party Providers ?**
  - To protect district's private data stored with provider
  - To mitigate risk of using provider
- **Who is involved in the vetting ?**
  - Curriculum Office
  - School Business Administrator/ Qualified Purchasing Agent
  - IT Leader
- **How do you protect your district & its data stored with 3rd Parties?**
  - By understanding 3rd Party Information Security Position
  - Requiring 3rd Party to share risk
  - Ensuring 3rd Party promptly notifies district of incident or breach

3rd Party Vetting & Contract Management

- **Favorite statements from vendors:**
  - “Our Software is FERPA Compliant!”
  - “We are School Officials”
- **Things that don’t exist:**
  - Official Department of Education FERPA Seal of Approval
  - Designating your vendor as a "School Official" places all risk on the district!

3rd Party Vetting & Contract Management

- **FERPA - Directory Information Exception:**
- Information in a student's education records that would not generally be considered harmful or an invasion of privacy if disclosed.
- This may include: Name, address, phone number, grade, photograph.
- Each institution determines their own directory policy which includes an opt out provision.
- Some institutions use a limited directory information policy that restricts who can receive directory data.

3rd Party Vetting & Contract Management

- **FERPA - School Official Exemption:**
  - Schools may disclose PII from education records without consent if the disclosure is to other school officials **within the school**, including faculty, whom the school has determined to have **legitimate educational interest**.
  - Schools may outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, teaching assistants, or other third parties provided **certain conditions are met**.

3rd Party Vetting & Contract Management

- **School Official Exemption – Conditions on Outsourcing:**
  - Performs an institutional service or function for which the agency or institution would otherwise use its employees;
  - Is under the **direct control of the agency or institution** with respect to the use and maintenance of education records;
  - PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;
  - Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.

3rd Party Vetting & Contract Management

- **FERPA Annual Notice**
  - Each institution has an annual notification of FERPA rights which includes criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.
  - The definition of a school official may vary from one institution to another.

3rd Party Vetting & Contract Management

- **Protecting Student, Privacy**
  - Student Privacy Laws:
    - Family Educational Rights & Privacy Act (FERPA) (31 Dec 1974)
    - Protection of Pupil Rights Amendment (PPRA) (6 Aug 1979)
    - Children's Online Privacy Protection Act (COPPA) (21 Apr 2000)
    - Children's Internet Protection Act (CIPA) (20 Apr 2001)
    - NJ Identity Theft Act (1 Jan 2006)
    - NJ Data Privacy Act (NJDPA) (15 Jan 2025)
  - Parent/Guardian Privacy Laws
    - Family Educational Rights & Privacy Act (FERPA) (31 Dec 1974)
    - NJ Identity Theft Act (1 Jan 2006)
    - NJ Data Privacy Act (NJDPA) (15 Jan 2025)
  - Staff Privacy Laws
    - NJ Identity Theft Act (1 Jan 2006)
    - NJ Data Privacy Act (NJDPA) (15 Jan 2025)

3rd Party Vetting & Contract Management

PACKAGED SOFTWARE REVIEW & APPROVAL

SOLUTION REVIEW AND APPROVAL

SPELL JIF SAFETY 360 RESOURCES

CASE STUDY – SOLUTION REVIEW

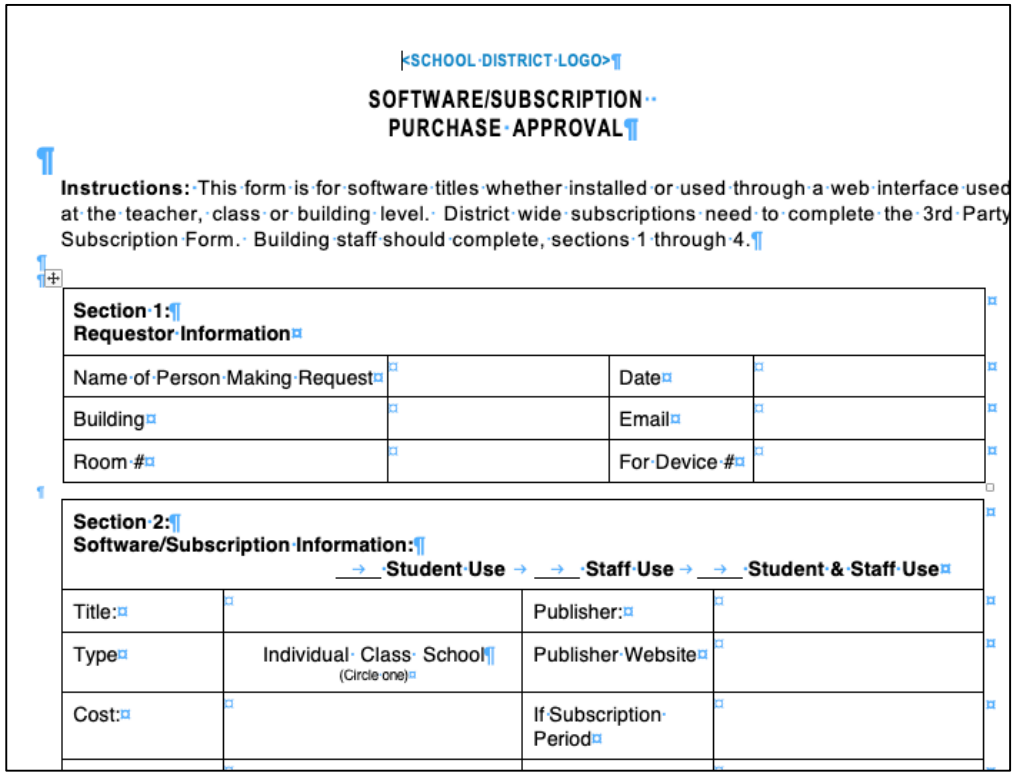
3rd Party Vetting & Contract Management

- **SPELL JIF Safety 360 Resources:**
  - Information Security Alert – 3rd Party Providers
  - 3rd Party Vetting Procedures/Guideline
  - Packaged Software or App Review Checklist
  - Solution Review Checklist
  - Contract – Bid/RFP Language to Protect District & Transfer Risk
  - Data Protection Addendum - Sample
- Case Study – Solution Review

3rd Party Vetting & Contract Management

- Packaged Software Review & Approval Form

- **Make sure to review:**
  - Terms of Service
  - Privacy Policy
  - How Accounts for Students under 13 are managed
  - Arbitration Clauses



<SCHOOL DISTRICT LOGO>

SOFTWARE/SUBSCRIPTION
PURCHASE APPROVAL

Instructions: This form is for software titles whether installed or used through a web interface used at the teacher, class or building level. District wide subscriptions need to complete the 3rd Party Subscription Form. Building staff should complete, sections 1 through 4.

Section 1: **Requestor Information**			
Name of Person Making Request		Date	
Building		Email	
Room #		For Device #	

Section 2: **Software/Subscription Information:** ___ **Student Use** ___ **Staff Use** ___ **Student & Staff Use**			
Title:		Publisher:	
Type	Individual Class School (Circle one)	Publisher Website	
Cost:		If Subscription Period	

3rd Party Vetting & Contract Management

Case Study – Solution Review – Attendance/Absence Solution

- Review with checklist designed by organization or district
- Purchase or engage a vendor to provide platform to conduct review.

3rd Party Vetting & Contract Management

Order Form- Review Solutions and Terms:

<School District Name>
<School Contact>
<School Contact Phone>
<School Contact Email>

Startup Cost Billing Terms: One – Time, Invoiced after signing
Subscription Frequency: Annual, Automatic Renewal
Sale Type: New
Initial Term: 04/01/24-06/30/25

Pricing Overview	**Amount**
One Time Fees	$ 22,700.00
Annual Recurring Fees	$ 38,445.50
Prorated Fees	$ 14,598.74

One Time Fee Description	**Quantity**	**Amount**
Implementation	1	$ 20,700.00
Import District Data	1	$ 2,000.00

Annual Fee Description	**Start Date**	**End Date**	**Amount**
HR Contract Portal	04/01/24	06/30/24	$ 11,730.93
HR Recruiting Solution	04/01/24	06/30/24	$ 2,867.81
HR Contract Portal	07/01/24	06/30/25	$ 26,942.75
HR Recruiting Platform	07/01/24	06/30/25	$ 11.502.75

3rd Party Vetting & Contract Management

Master Services Agreement or Terms of Service - 15 Page document refers to attachments representing another 32 pages of other documents. 47 pages that you acknowledge and accept when you click to accept the order form!

The terms are subject to change and posted online, you the district need to monitor them to determine if your contractual rights are changed.

3rd Party Vetting & Contract Management

Review of Terms:

will act as a data processor, and will act on Client's instruction, as specified in the Order Form, concerning the treatment of Personal Data provided in connection with the Subscription Software and Services. Client shall provide all notices and obtain all consents (including consent of any parent or guardian for any minor) required for Client's use of the Subscription Software and receipt of the Services, and Company Name's provision of the Subscription Software and Services, including those related to the collection, use, storage, processing, transfer, and disclosure of Personal Data. Client agrees that it must properly enter data, information, and other Client Content and configure settings within the Subscription Software for the Subscription Software to operate properly. Client shall verify the accuracy of the Client Content

Company is fixing the district to be responsible for PII including obtaining and managing consent for student Records.

3rd Party Vetting & Contract Management

Review of Terms

completeness, legality, use of, or reliance on the Client Content. Client assumes the sole responsibility for the selection of the Subscription Software and Services to achieve Client's intended results, the use of the Subscription Software and Services, and the results attained from such selection and use.¶

Company terms Client or School District has sole responsibility or Subscription... So if product does not work or meet your needs, it's you fault.

3rd Party Vetting & Contract Management

Review of Terms

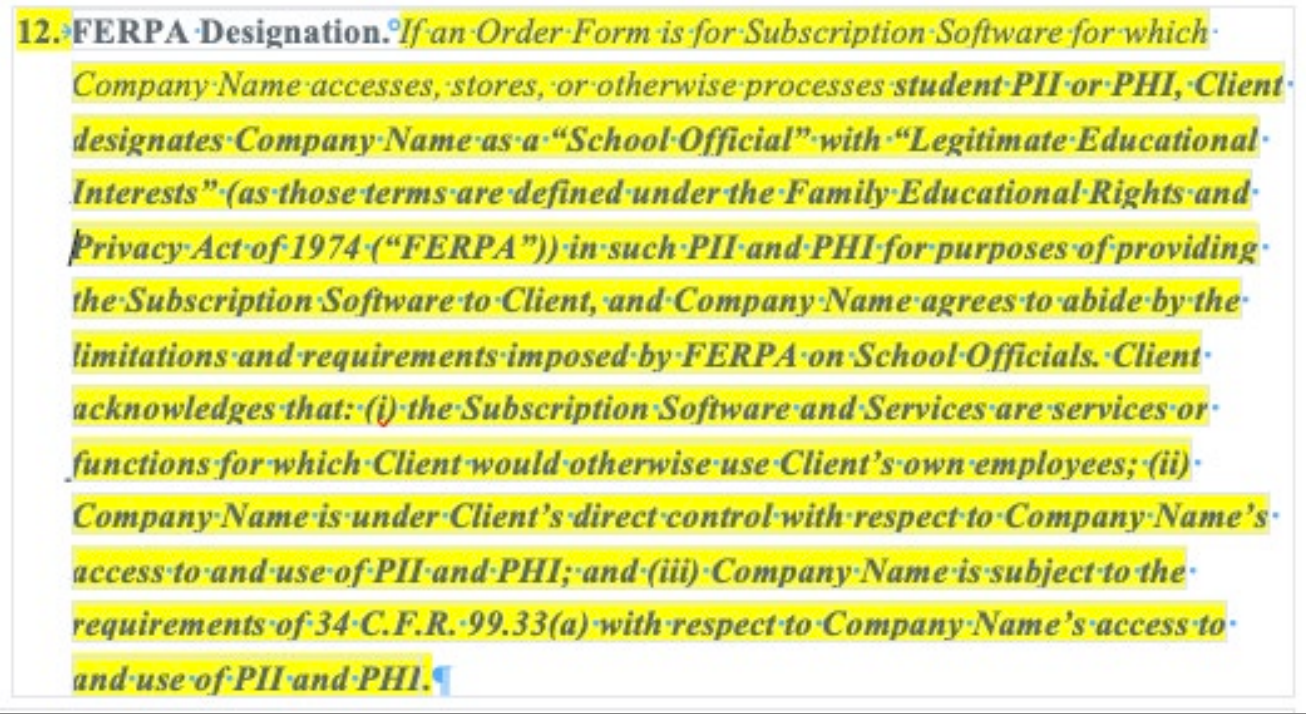
11. **Client Responsibilities.** Client agrees that (a) Client shall have **sole** responsibility for administering access security to the Subscription Software for its Authorized Users; (b) Client shall review any output resulting from its use of the Subscription Software and confirm that such output is correct; and (c) if Client uses the Software for reimbursement or payment from Medicaid or other government agencies, Company Name shall have **no responsibility**, and Client shall have **sole responsibility**, to submit information and claims for such reimbursement or payment. Company Name **does not warrant that the Subscription Software, or the results derived therefrom, will meet Client's requirements, or that the operation of the Subscription Software will be uninterrupted or error-free.** Client is **solely** responsible for obtaining and maintaining, at its own expense, all hardware, software, and services needed to access and use the Subscription Software, including any and all servers, computers, and Internet access services. In connection with the performance of the Services, Client shall provide Company Name's personnel with all such cooperation and assistance as they may reasonably request, or otherwise may reasonably be required, to enable Company Name to perform its obligations, and exercise its rights, under and in accordance with the terms and conditions of this Agreement.

Look for this clause in all contracts, terms and agreements - this is where the provider will fix your responsibility. If any of these terms is not acceptable, an addendum will need to be signed. Note the bold, there is "**no guarantee the services will work, be error free.**"

PS: There is no section for Company responsibilities!

3rd Party Vetting & Contract Management

Review of Terms



12. **FERPA Designation.** *If an Order Form is for Subscription Software for which Company Name accesses, stores, or otherwise processes student PII or PHI, Client designates Company Name as a "School Official" with "Legitimate Educational Interests" (as those terms are defined under the Family Educational Rights and Privacy Act of 1974 ("FERPA")) in such PII and PHI for purposes of providing the Subscription Software to Client, and Company Name agrees to abide by the limitations and requirements imposed by FERPA on School Officials. Client acknowledges that: (i) the Subscription Software and Services are services or functions for which Client would otherwise use Client's own employees; (ii) Company Name is under Client's direct control with respect to Company Name's access to and use of PII and PHI; and (iii) Company Name is subject to the requirements of 34 C.F.R. 99.33(a) with respect to Company Name's access to and use of PII and PHI.*

Look for this clause in all contracts, terms and agreements - this is where the provider will require you to designate them as a "school official" and require you the subscriber to be responsible for their actions! There is federal legislation pending to prevent companies from doing this.

3rd Party Vetting & Contract Management

Review of Terms

terminated in accordance with this Agreement, and, to the extent permitted by applicable law, will automatically renew for successive one-year terms thereafter (each, a "**Renewal Term**"), subject to fee increases for Renewal Terms in accordance with Section 2 above, unless one party notifies the other party of non-renewal in writing at least 60 days prior to the end of the current Order Form Initial Term or Renewal Term. In the event notice of a price increase in section 2 is not

3. **No Termination for Convenience.** Client is not entitled to terminate this agreement for any reason other than those contained in this Agreement. No termination for convenience is permitted.

Watch for auto-renewal clauses, while School PO's generally have an adequate appropriation clause, this will result in you paying another year of fees if not removed or if notice is not timely. No termination for convenience.

3rd Party Vetting & Contract Management

Review of Terms

2. **Data Security.** Company Name will utilize commercially reasonable administrative, technical, and physical measures designed to maintain the confidentiality and security of Personal Data submitted by Client into the Subscription Software or otherwise provided to Company Name. Client understands and agrees that no security measures can be 100% effective or error-free and understands that Company Name expressly disclaims (a) any warranty that these security measures will be 100% effective or error-free or (b) any liability related to the confidentiality and security measures utilized by third parties.

Company will take “Commercially Reasonable” – which is not defined anywhere in the agreements or it attachments. There is NO Warranty, the security measures will be effective or error free. This disclaimer takes the company and its third party processers off the hook and puts the district on the hook. If you are hosting PII, PHI, Student Data or Financial Data you may want a definition of the phrase “Commercially Reasonable”

3rd Party Vetting & Contract Management

Review of Terms

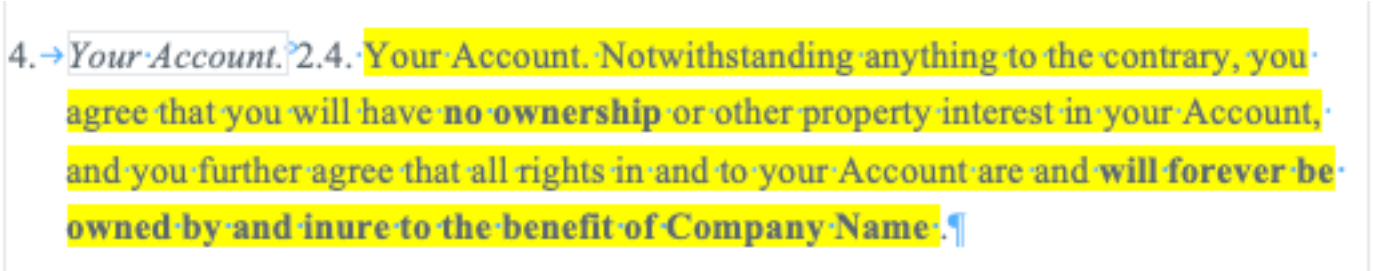
1. *Applicability of Arbitration Agreement.* You agree that any dispute, claim, or request for relief relating in any way to your access or use of the Company Name Technology, or to any aspect of your relationship with Company Name, will be resolved by **binding arbitration,** rather than in court, except that (1) you may assert

2. *Arbitration Rules and Forum.* The Federal Arbitration Act governs the interpretation and enforcement of this Arbitration Agreement. To begin an arbitration proceeding, **you must send a letter requesting arbitration and describing your dispute or claim or request for relief to our registered agent, The Corporation Trust Company, at Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801**. The arbitration will be conducted by JAMS, an

All disputes must be settled by Arbitration – in Delaware

3rd Party Vetting & Contract Management

Review of Terms

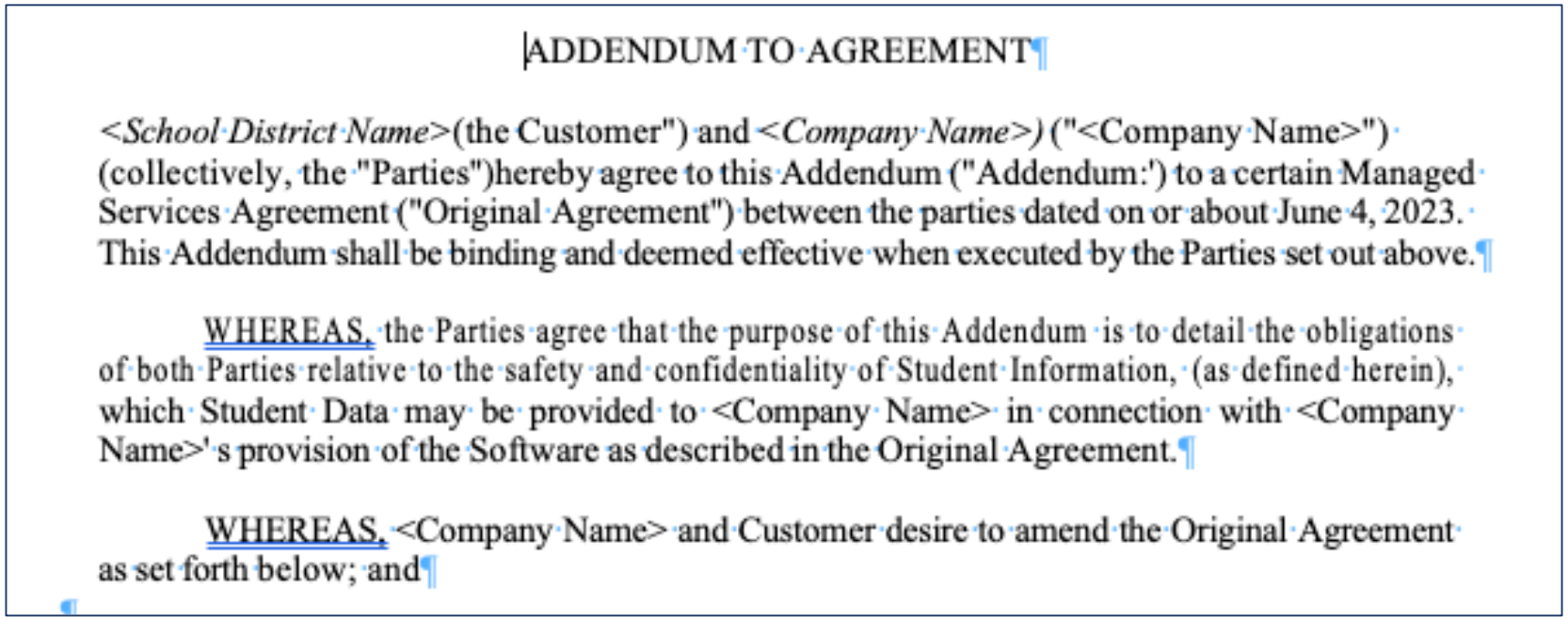

4. *Your Account.* 2.4. Your Account. Notwithstanding anything to the contrary, you agree that you will have **no ownership** or other property interest in your Account, and you further agree that all rights in and to your Account are and **will forever be owned by and inure to the benefit of Company Name**.

You do not own your account to access this subscription ….

3rd Party Vetting & Contract Management

Will companies make a change ?

Some will, this company when pressed will sign an addendum, it takes a long time to get them to agree and an attorney who will fight to protect the district's interests.



ADDENDUM TO AGREEMENT

<*School District Name*>(the Customer") and <*Company Name*>) ("<Company Name>") (collectively, the "Parties")hereby agree to this Addendum ("Addendum:') to a certain Managed Services Agreement ("Original Agreement") between the parties dated on or about June 4, 2023. This Addendum shall be binding and deemed effective when executed by the Parties set out above.

WHEREAS, the Parties agree that the purpose of this Addendum is to detail the obligations of both Parties relative to the safety and confidentiality of Student Information, (as defined herein), which Student Data may be provided to <Company Name> in connection with <Company Name>'s provision of the Software as described in the Original Agreement.

WHEREAS, <Company Name> and Customer desire to amend the Original Agreement as set forth below; and

3rd Party Vetting & Contract Management

What happens when they will not modify terms ?

1. Select another solution
2. Purchase additional solutions take steps procedurally to address issues.

Panel Discussion Questions & Answers

Thank you for Attending!

Enjoy Lunch

All Presentations will be posted on SPELLJIF.COM website

Model Notification of Rights under FERPA for Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students who are 18 years of age or older ("eligible students") certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of school ("School")] receives a request for access.

   Parents or eligible students who wish to inspect their child's or their education records should submit to the school principal [or appropriate school official] a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.

2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

   Parents or eligible students who wish to ask the [School] to amend their child's or their education record should write the school principal [or appropriate school official], clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.

3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. The criteria for determining who constitutes a school official and what constitutes a legitimate educational interest must be set forth in the school's or school district's annual notification for FERPA rights. A school official typically includes a person employed by the school or school district as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer, contractor, or consultant who, while not employed by the school, performs an institutional service or function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, medical consultant, or therapist;

a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks. A school official typically has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

[Optional] Upon request, the school discloses education records without consent to officials of another school or school district in which a student seeks or intends to enroll, or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer. [NOTE: FERPA requires a school or school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request or the disclosure is initiated by the parent or eligible student.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The name and address of the Office that administers FERPA are:

   Student Privacy Policy Office
   U.S. Department of Education
   400 Maryland Avenue, SW
   Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by § 99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that elementary and secondary schools may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in § 99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, § 99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student –

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in § 99.31(a)(1)(i)(B)(*1*) - (a)(1)(i)(B)(*3*) are met. (§ 99.31(a)(1))

- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already

enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of § 99.34. (§ 99.31(a)(2))

- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the State educational agency (SEA) in the parent or eligible student's State. Disclosures under this provision may be made, subject to the requirements of § 99.35, in connection with an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf, if applicable requirements are met. (§§ 99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary for such purposes as to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§ 99.31(a)(4))

- To State and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a State statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to § 99.38. (§ 99.31(a)(5))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction, if applicable requirements are met. (§ 99.31(a)(6))

- To accrediting organizations to carry out their accrediting functions. (§ 99.31(a)(7))

- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§ 99.31(a)(8))

- To comply with a judicial order or lawfully issued subpoena if applicable requirements are met. (§ 99.31(a)(9))

- To appropriate officials in connection with a health or safety emergency, subject to § 99.36. (§ 99.31(a)(10))

- Information the school has designated as "directory information" if applicable requirements under § 99.37 are met. (§ 99.31(a)(11))

- To an agency caseworker or other representative of a State or local child welfare agency or tribal organization who is authorized to access a student's case plan when such agency or organization is legally responsible, in accordance with State or tribal law, for the care and protection of the student in foster care placement. (20 U.S.C. § 1232g(b)(1)(L))

- To the Secretary of Agriculture or authorized representatives of the Food and Nutrition Service for purposes of conducting program monitoring, evaluations, and performance measurements of programs authorized under the Richard B. Russell National School Lunch Act or the Child Nutrition Act of 1966, under certain conditions. (20 U.S.C. § 1232g(b)(1)(K))

Third Party Vendor Vetting Checklist

To make sure that the vendor can properly and safely integrate into the districtwide applications, the vendor must meet the following requirements based on the security level of the shared data.

Local Education Agency:

Vendor Name:

Product:

Contract Period:

Phase I: Vendor Selection

- ☐ The vendor, if software as a service, has been told by the LEA they will need to provide the security documents to the LEA initially and on an annual basis.

Phase II: Data Collection

- ☐ The LEA systems they will be connecting to (List Systems i.e. Powerschool, Genesis, Systems 3000, CSI, etc.))
- ☐ The method of integration (API, SFTP, etc.)
- ☐ Specific data fields requested and the rationale for their inclusion in the request, including how the data will be used in the target system.
- ☐ A description of how data will be restricted to the users who have a legitimate business need to see the data.
- ☐ The vendor has provided the following, or links to the following:
  - Terms or Service, Master Service Agreement, Service Level Agreement
  - Privacy Policy
  - Data Security Policy
- ☐ A description of how data will be restricted to the users who have a legitimate business need to see the data.

The vendor has provided the LEA the following security documentation:

- ☐ The Vendor Readiness Assessment (VRA) to capture the baseline security controls.
- ☐ A third-party conducted assessment reports such as the SOC 2 Type 2 audit, ISO 27001 certification, initially and then annually.

Phase III: Evaluation

Does the vendor have gaps indicated in their internal controls (from the VRA)?

- ☐ No
- ☐ Yes, and we have requested the following additional documentation and mitigating controls:
  - ☐ A credentialed vulnerability scan to be provided at execution of the contract and annually thereafter, showing no medium or above vulnerabilities.
  - ☐ A third-party penetration test to be provided at execution of the contract and annually thereafter, showing no medium or above findings.

  Other:
  - ☐ A contract addendum to address Data Protection.
  - ☐ A contract addendum to address Data Security.
  - ☐ Other_____

Phase IV: Contract Award

- ☐ The LEA has executed the Vendors Standard Agreement.
- ☐ The LEA has executed an Addendum to the standard Agreement as noted above.

_____ _____

Approved by: < Technology Director Name> Date

<Technology Director Title>

CYBERSECURITY CONTRACT REVIEW GUIDANCE DOCUMENT

Effective contract review requires a process in place that defines how a review will be conducted to quantify the risk of entering a specific contract. It is also a process to allow a district to share the cyber liability with its 3rd party providers of hardware, software and other solutions used to support the administrative functions of the school district and provide instructional solutions to support the instructional goals of the district.

School Districts should have a policy for Data Protection and Classification, which sets forth the requirements for storing, transmitting, and sharing public, internal, and confidential within the district and with 3rd Party Providers.

In addition to proper review and vetting of third-party providers, the district should have a process to ensure appropriate language in included in bid or request for proposal documents and the contract that is signed with 3rd Party Providers for the hardware or software solutions they are providing.

It is essential schools define the incremental risk to the school district when engaging third-party IT service providers as well as defining a due diligence process for mitigating those risks - third-party risk from remote access, data transmission and offsite storage.

Consider the following as an outline for a contract monitoring process:

1. **System Procurement Process**
    1. Identify the individual(s) responsible for monitoring the contract. Usually, the IT Manager or School Business Administrator.
    2. During development of bid or request for proposal documents:
        1. Assess the readiness of the 3rd Party Vendor in meeting the district's security requirements, and provide clear, concise definition in those documents of what the district expects of the vendor.
        2. Identify new security requirements that may arise during the contract.
    3. If applicable, perform a review or request audit of vendor security practices and procedures and/or perform penetration test.
2. **Post Procurement**
    1. Follow up
        1. Require IT Manager or School Business Administrator to perform a risk assessment based on Data Protection policy

(annually if confidential data is involved or every 3 years for internal or public data.

2. Review the risk assessment results. Any concerns? Any problems? Any unknowns that need to be addressed with the vendor?

2. Follow up with vendor. Access logs available? Any pending items resolved? Are things on their end as expected? Any owner concerns?

3. Based on risk (annually or tri-annually), resubmit third-party information security risk assessment to assess what has changed, what needs closer scrutiny, or identify inconsistencies with previous assessments

4. Establish a working relationship with your vendor.

5. Review security incidents involving the system/application/process. Are these due to non-compliance?

6. If applicable, based on the contract, require subsequent assurance tests.

Sample RFP/Bid – Contract Clauses

Assistance With Litigation

Sample RFP Language:

1. Describe the procedures and methodology in place to retain, preserve, backup, delete, and search data in a manner that meets the requirements of electronic discovery rule.

Sample Contract Clauses:

1. [Vendor] shall make itself and any employees, subcontractors, or agents assisting [Vendor] in the performance of its obligations under the Agreement available to <School District> at no cost to <School District> to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against <School District> , its officers, agents or employees based upon a claimed violation of laws relating to security and privacy and arising out of this Agreement.

2. E-Discovery: "The obligations of this Section ___ shall not act to restrict [Vendor]'s lawful disclosure of the <School District> Data pursuant to any applicable state or federal laws or by request or order of any court or government agency. Provided, however, before making such a disclosure, [Vendor] must give <School District> and all affected employees prior written notice of that disclosure, which must identify: the data [Vendor] intends to disclose, the law(s), request, or order under which [Vendor] believes it is required to make such a disclosure, the persons or entities to whom [Vendor] intends to disclose such data, and the date on which [Vendor] is required to make such a disclosure."

3. E-Discovery: "In order to provide <School District> with the ability to be compliant with e-discovery rules, [Vendor] must provide the following where "relevant data" might include any data stored regarding any person affiliated with <School District> , access logs, activity logs, transaction logs, changes to access rights, etc., as detailed by the system architecture and practices provided by [Vendor].

    1. Up-to-date documentation of its system architecture, operating practices, especially as regards data retention, backups, and data deletion, and other potentially relevant data sufficient to enable <School District> to accurately represent what [Vendor] can and cannot produce for discovery purposes. <School District> will provide a template upon request.

    2. Suspension of any routine destruction of potentially relevant data upon receiving written notice and as instructed by <School District> until such time as the suspension is released in writing by <School District> . A snapshot of all available potentially relevant data (including data on prior-backup media) may be acceptable provided that newly created/updated data is suitably preserved on an on-going basis and little risk of modifying or losing data or metadata exists.

3. Preservation of potentially relevant data in its native form, including any metadata, upon receiving written notice and as instructed by <School District> until such time as the suspension is released in writing by <School District> . A snapshot of all available potentially relevant data (including data on prior-backup media) may be acceptable provided that newly created/updated data is suitably preserved on an on-going basis and little risk of modifying or losing data or metadata exists.

4. Search capability to assist in identifying potentially relevant data. Searchable data will be determined by analysis of the system architecture provided by [Vendor]. Search results must be deliverable within a reasonable time period provided by written notice and instruction by <School District> .

5. Produce potentially relevant data in both native and humanly-readable forms, including any metadata, understanding that [Vendor] stores all data in a proprietary, encrypted format, upon written notice, in accordance with the timeframe specified in the notice and as instructed by <School District> . Production may be accomplished via electronic file transfer or as physical media so long as metadata is preserved.

6. Compliance with requests to testify as to the application architecture, operating practices, and procedures followed in preservation or production activities, and other questions that may arise in the course of litigation.

Credit Card Data

Sample RFP Language:

1. Does the Proposer conform to and meets PCI DSS standards? If yes, provide examples of Proposer practices that can assist with our understanding of how the Proposer meets PCI standards.

2. Does the Proposer monitor the PCI DSS standards and the Proposer's own information security practices to ensure continued compliance? If yes, describe the Proposer's monitoring activities and their frequency.

3. Would the Proposer be willing to provide a letter of certification or independent audit report to attest to meeting PCI DSS standard requirements? If no, Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.

Sample Contract Clauses:

1. The VENDOR certifies that their Information Technology practices conform to and meet PCI DSS standards as defined by major credit card vendors Visa and MasterCard at https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html and https://www.mastercard.us/en-us/business/overview/safety-and-security/security-recommendations/site-data-protection-PCI/merchants-need-to-know.html The Vendor will monitor these PCI DSS standards and its Information Technology practices and the Vendor will notify the District within one (1) week, if its practices should not conform to such standards. The VENDOR will provide a letter of certification to attest to meeting this requirement.

2. "Contractor agrees that it may (1) create, (2) receive from or on behalf of district , or (3) have access to, payment card records or record systems containing cardholder data including credit card numbers (collectively, the "Cardholder Data"). Contractor shall comply with the Payment Card Industry Data Security Standard ("PCIDSS") requirements for Cardholder Data that are prescribed by Visa, as they may be amended from time to time (collectively, the "PCIDSS Requirements"). Contractor acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by Visa, for purposes of this Agreement or as required by applicable law."

Data Definition

Sample RFP Language:

The following language should the lead-in paragraph to an Information Security section.

1. For the purpose of this RFP, Confidential records or information are defined as any and all information owned by <School District> - created, received from or on behalf of <School District> , or accessed in the course of performing the [service] - of which collection, disclosure, protection, and disposition is governed by state or federal law or regulation, particularly information subject to [Enter Applicable Laws here.] This information includes, but is not limited to, [Enter list of applicable data items in here].

2. For this RFP, <School District> records [data] are defined as any and all data created, received from or on behalf of <School District> , or accessed in the course of performing the [service] including, but not limited to, [Enter list of applicable data items in here]. <School District> records also include all information, including personally identifiable information, derived from other <School District> records.

Sample Contract Clauses:

1. For purposes of this addendum, Confidential Information is defined as any and all information whose collection, disclosure, protection, and disposition is governed by state or federal law or regulation, particularly information subject to the Family Educational Rights and Privacy Act (FERPA), or [insert state law code sections here as applicable]. This information includes, but is not limited to, Social Security

Numbers, student records, financial records regarding students (or their parents), financial and personal information regarding <School District> employees, and other personally identifiable information identified by law.

2. Define "Confidential <School District> Data" as any data or information owned by <School District> that [Vendor] creates, obtains, accesses (via records, systems, or otherwise), receives (from <School District> or on behalf of the <School District>), or uses in the course of its performance of the contract which include, but not be limited to: social security numbers; credit card numbers; any data protected or made confidential or sensitive by the Family Educational Rights and Privacy Act, as set forth in 20 U.S.C. §1232g ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 and the federal regulations adopted to implement that Act (45 CFR Parts 160 & 164 "the HIPAA Privacy Rule"), collectively referred to as "HIPAA", or any other applicable federal or [State] law or regulation.

Data Protection After Contract Termination

Sample RFP Language:

1. What procedures and safeguards does the Proposer have in place for sanitizing and disposing of <School District> data according to prescribed retention schedules or following the conclusion of a project or termination of a contract to render it unrecoverable and prevent accidental and/or unauthorized access to <School District> data?

Sample Contract Clauses:

1. The [Vendor] agrees that at the termination of this contract, all <School District> data will be either returned to the <School District> or destroyed as indicated by the <School District> at the time of contract termination.

2. Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return all [term for confidential data] to <School District> or, if return is not feasible, destroy all [term for confidential data].

3. Within 30 days after the termination or expiration of a Purchase Order, Contract or Agreement for any reason, [Vendor] shall either: Return or destroy, as applicable, all confidential data provided to the [Vendor] by <School District> to [Vendor], including all confidential data provided to [Vendor]'s employees, subcontractors, agents, or other affiliated persons or entities; or In the event that returning or destroying the confidential data is not feasible, provide notification of the conditions that make return or destruction not feasible, in which case, the [Vendor] must continue to protect all confidential Data that it retains and agree to limit further uses and disclosures of such Data to those purposes that make the return or destruction not feasible as [Vendor] maintains such Data.

4. The [Vendor] agrees, upon termination, cancellation, expiration, or other conclusion of this Agreement, within 30 days to return to the <School District> or if return is not feasible, destroy and not retain any copies (and furnish the <School District> with an appropriate Certificate of Destruction) of any and all Confidential Information that is in its possession.

5. Upon termination, cancellation, expiration or other conclusion of the Agreement, [Vendor] shall return the Covered Data to <School District> unless <School District> requests that such data be destroyed. This provision shall also apply to all Covered Data that is in the possession of subcontractors or agents of [Vendor]. [Vendor] shall complete such return or destruction not less than thirty (30) days after the conclusion of this Agreement. Within such thirty (30) day period, [Vendor] shall certify in writing to <School District> that such return or destruction has been completed.

6. At the completion of this agreement, [Vendor] will physically or electronically destroy beyond all ability to recover all <School District> data provided to them. This includes any and all copies of the data such as backup copies created at any [Vendor] site.

7. End of Agreement Data Handling. The [Vendor] also agrees that upon termination of this Agreement it shall erase, destroy, and render unreadable all <School District> data according to the standards enumerated in D.O.D. 5015.2 and certify in writing that these actions have been complete within 30 days of the termination of this Agreement or within 7 days of the request of an agent of <School District> , whichever shall come first.

8. Upon request by Customer made before or within sixty (60) days after the effective date of termination, [Vendor] will make available to Customer for a complete and secure (i.e. encrypted and appropriated authenticated) download file of Customer Data in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. [Vendor] will be available throughout this period to answer questions about data schema, transformations, and other elements required to fully understand and utilize Customer's data file. After such sixty (60) day period, [Vendor] and its hosted service provider shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, delete in such a manner as prevents recovery through normal/laboratory means, all Customer Data in its systems or otherwise in its possession or under its control.

Data Sharing

Sample RFP Language:

1. What administrative safeguards and best practices does the Proposer have in place to vet Proposer's and third parties' staff members that would have access to the environment hosting all systems that would interact with the service proposed

including any systems that would hold, process, or from which <School District> data may be accessed to ensure need-to-know-based access.

2. Describe the Proposer's password policy including password strength, password generation procedures, and frequency of password changes. If passwords are not used for authentication to the proposed system, describe what alternative controls are used to manage user access.

3. How will users authenticate to the proposed system? What procedures and best practices does the Proposer have in place to ensure that user credentials are updated and terminate as required by changes in role, responsibilities, and employment status.

4. Does the product provide the capability to use local credentials (i.e., federated authentication) for user authentication and login. If yes, describe how the product provides that capability.

5. Does the product manage administrator access permissions at the virtual system level? If yes, describe how this is done.

Sample Contract Clauses:

1. Except as otherwise specifically provided for in this Agreement, the [Vendor] agrees that <School District> data will not be shared, sold, or licensed with any third-party, except for approved sub-contractors, without the express approval of the <School District> through a data letter agreement.

2. The [Vendor] certifies that only employees of the company or approved contractors will be granted access to <School District> data.

3. [Vendor] shall represent, warrant, and certify it will: Hold all Confidential Datain the strictest confidence; Not release any Confidential Dataconcerning an <School District> student unless [Vendor] obtains <School District> 's prior written approval and performs such a release in full compliance with all applicable privacy laws, including FERPA.

4. [Vendor] agrees to hold any and all Confidential Information obtained from the <School District> , its students, faculty, staff, or other agents in the performance of this Agreement in strictest confidence and shall not use or disclose such Confidential Information except as permitted or required by this Agreement or by law or as otherwise agreed to in writing by the <School District> .

5. Access to <School District> Data must be strictly controlled and limited to [Vendor] staff assigned to this project on a need-to-know basis only.

6. [Vendor] agrees to hold [term for sensitive data] in strict confidence. [Vendor] shall not use or disclose [term for sensitive data] received from or on behalf of <School District> except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by <School District> . [Vendor] agrees that it will protect the [term for sensitive data] it receives from or on behalf of <School District> according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

7. [Vendor] agrees to hold Covered Data received from or created on behalf of <School District> in strictest confidence. [Vendor] shall not use or disclose Covered Data except as permitted or required by the Agreement or as otherwise authorized in writing by <School District> . If required by a court of competent jurisdiction or an administrative body to disclose Covered Data, [Vendor] will notify <School District> in writing prior to any such disclosure in order to give <School District> an opportunity to oppose any such disclosure. Any work using, or transmission or storage of, Covered Data outside the United States is subject to prior written authorization by the <School District> .

Data Transmission (including Encryption)

Sample RFP Language:

1. How does <School District> data go between <School District> and Proposer's proposed system? If connecting via a private circuit, describe what security features are incorporated into the private circuit. If connecting via a public network (e.g., the Internet), describe the way the Proposer will safeguard <School District> data.

2. Does the product secure the data transmission between <School District> and the Proposer? If yes, describe how the Proposer provides that security. If no, what alternative safeguards are used to protect <School District> data in transit?

3. Does the product secure the communications between the managed systems or administrators to the centralized manager server? If yes, describe how the product provides that security.

4. Does the product encrypt Confidential data in transit and at rest? If yes, describe how the product provides that security. If no, what alternative methods are used to safeguard Confidential data in transit and at rest?

5. Does the Proposer protect <School District> data backups against unauthorized access? If yes, describe the methods used by the Proposer to provide that protection.

6. Does the Proposer encrypt <School District> data backups? If yes, describe the methods used by the Proposer to encrypt backup data. If no, what alternative

safeguards does the Proposer use to protect <School District> data backups against unauthorized access?

Sample Contract Clauses:

1. [Vendor] agrees that any transfer of data between the <School District> and [Vendor] or within [Vendor]'s computing environment will take place using encrypted protocols such as SSL, step or scup.

2. [Vendor] certifies that all data backups of the <School District> 's data will be stored and maintained in an encrypted format using at least a 128 bit key.

3. [Vendor] will use only secure methods to access and electronically transfer <School District> data files such as Secure or Securest from the <School District> location and the [Vendor] location.

4. [Vendor] will use all reasonable practices and security procedures necessary to protect all electronic data that is transmitted between those parties under this Agreement by (but not limited to) electronic transmission or the physical delivery of electronically recorded data. Such protective measures shall include, but not be limited to, use of up-to-date anti-virus software to guard against viruses, worms, Trojan horses, or other malware that may permit unauthorized access to data or may compromise the confidentiality, integrity or authorized accessibility of data or associated information systems of the other party. Neither <School District> nor [Vendor] shall introduce into electronic data transmitted between them under this Agreement any virus, worm, Trojan horse, or other malware that may permit unauthorized access to data or may compromise the confidentiality, integrity or authorized accessibility of data or associated information systems of the other party. Provided, however, in no event shall <School District> be responsible for any damages or loss caused by electronic data transmitted to [Vendor].

Financial Information

Sample RFP Language:

1. Proposer may create, receive from or on behalf of <School District>, or have access to financial records. Describe the security features incorporated into the product to safeguard records.

Sample Contract Clauses:

1. [Vendor] agrees that it will execute an agreement with the <School District> to set forth it’s responsibilities for safeguarding district financial data.

General Data Protection

Sample RFP Language:

1. Describe the security features incorporated into the product.

2. List all products, including imbedded products, in the proposal and their corresponding owning company. **Note**: This is what could be called "potential security problems by proxy." This question can also be included in a product architecture-related section.

3. Does the Proposer have an Information Security Plan, supported by security policies and procedures, in place to ensure the protection of information and information resources? If yes, describe the outline of the Plan and how often it is updated. If no, describe what alternative methodology the Proposer uses to ensure the protection of information and information resources.

4. Describe the monitoring procedures and tools used for monitoring the integrity and availability of the systems interacting with the service proposed, detecting security incidents, and ensuring timely remediation.

5. Describe the physical access controls used to limit access to the Proposer's data center and network components only to [Enter appropriate list here].

6. List the Proposer's staff members and third-party entities, and corresponding roles, that would have access to the environment hosting all systems that would interact with the service proposed including any systems that would hold, process, or from which <School District> data may be accessed.

7. What additional administrative, technical, and physical security controls does the Proposer have in place or plan to put in place?

8. What procedures and best practices does the Proposer follow to harden all systems that would interact with the service proposed including any systems that would hold, process, or from which <School District> data may be accessed?

9. What technical security measures does the Proposer take to detect and prevent unintentional [accidental] and intentional corruption or loss of <School District> data?

10. Does the Proposer have a process for security quality assurance testing of the systems interacting with the service proposed? If yes, describe the activities designed to validate the security architecture and functionality.

11. Describe any assumptions made in the preparation of your proposal regarding information security outside those already supplied by your company in the proposal.

12. Proposer may create, receive from or on behalf of <School District> , or have access to records or record systems that contain social security numbers (SSN). Describe the security features incorporated into the product to safeguard SSNs. **Note:** The same question may be used for credit cards and other known sensitive data.

13. Does the proposed solution use a public-key based digital signature as required under [Enter applicable law/directive here]. If yes, describe how the product meets such requirement. If no, what alternatives does the Proposer use to meet such requirement. **Note:** This is for security solutions that use a Public Key Infrastructure (PKI)

14. Does the proposed solution use digital certificates from a PKI Service Provider that appears in the "Approved List of PKI Service Providers" [Enter list link here]. If no, what alternatives does the Proposer use to meet such requirement. **Note:** This is for security solutions that use a Public Key Infrastructure (PKI)

Sample Contract Clauses:

1. [Vendor] shall develop, implement, maintain, and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted [term for sensitive data] received from, or on behalf of <School District> or its students. These measures will be extended by contract to all subcontractors used by [Vendor].

2. The [Vendor] agrees that it will protect the Confidential Information it receives according to commercially acceptable standards and no less rigorously than it protects its own Confidential Information. Specifically, the [Vendor] shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentially, integrity, and availability of all electronically managed Confidential Information.

3. [Vendor] agrees that it will protect the Covered Data according to commercially acceptable standards and no less rigorously than it protects its own confidential information, but in no case less than reasonable care. [Vendor] shall develop, implement, maintain and use appropriate administrative, technical and physical security measures which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all such Covered Data.

4. It is the responsibility of [Vendor] to ensure that all possible measures have been taken to secure the computers or any other storage devices used for <School District> data. This includes industry-accepted firewalls, up-to-date anti-virus software, controlled access to the physical location of the hardware itself, etc.

5. <School District> shall reserve the right to change or modify without consent any <School District> information resource, including but not limited to operating systems, hardware, and/or network configuration, to protect <School District> information resources against any security vulnerabilities and unauthorized access or abuse.

6. SSN Specific: [Vendor] agrees that it may (1) create, (2) receive from or on behalf of <School District> , or (3) have access to, records or record systems containing social security numbers (collectively, the "SSN Records"). [Vendor] represents, warrants, and agrees that it will: (1) hold the SSN Records in strict confidence and will not use or disclose the SSN Records except as (a) permitted or required by this Agreement, (b) required by law, or (c) otherwise authorized by <School District> in writing; (2) safeguard the SSN Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which [Vendor] protects its own confidential information; and (3) continually monitor its operations and take any action necessary to assure that the SSN Records are safeguarded in accordance with the terms of this Agreement. At the request of <School District> , [Vendor] agrees to provide <School District> with a written summary of the procedures [Vendor] uses to safeguard the SSN Records.

7. Data Storage. [Vendor] also agrees that any and all <School District> data will be stored, processed, and maintained solely on designated target servers and that no <School District> data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the [Vendor]'s designated backup and recovery processes.

Indemnification as a Result of Security Breach

Sample RFP Language:

- Not Applicable. Best addressed with contract clauses.

Sample Contract Clauses:

1. [Vendor] shall defend and hold <School District> harmless from all claims, liabilities, damages, or judgments involving a third party, including <School District> 's costs and attorney fees, which arise because of [Vendor]'s failure to meet any of its obligations under this contract.

2. [Vendor] shall indemnify, defend and hold <School District> harmless from all lawsuits, claims, liabilities, damages, settlements, or judgments, including <School District> 's costs and attorney fees, which arise because of [Vendor]'s negligent acts or omissions or willful misconduct.

Notification of Security Incidents

Sample RFP Language:

1. Describe what procedures the Proposer has in place to isolate or disable all systems that would interact with the service proposed in case a security breach should be identified? Including any systems that would hold, process, or from which School district data may be accessed.

2. What procedures, methodology, and timetables does the Proposer have in place to detect information security breaches and notify School district, and customers? [Include definition of security breach if it has not been defined in the RFP Definitions section already.]

3. Describe the procedures and methodology in place to detect information security breaches and notify customers in a manner that meets the requirements of the state breach notification law.

Sample Contract Clauses:

1. The [Vendor] agrees to notify the University when any [Vendor] system that may access, process, or store School district data is subject to unintended access. Unintended access includes compromise by a computer worm, search engine web crawler, password compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures. [Vendor] further agrees to notify the school district within twenty-four (24) hours of the discovery of the unintended access by providing notice via email to [email address, typically security office or IT Manager].

2. [Vendor] agrees to notify the school district of within XX minutes/hours if there is a threat to [Vendor]'s product as it pertains to the use, disclosure, and security of the school district's data.

3. If an unauthorized use or disclosure of any Confidential Dataoccurs, [Vendor] must provide: Written notice within one (1) business day after [Vendor]'s discovery of such use or disclosure and all information School district requests concerning such unauthorized use or disclosure.

4. [Vendor], within one day of discovery, shall report to School district any use or disclosure of [term for sensitive data] not authorized by this Addendum or in writing by School district. [Vendor]'s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the [term for sensitive data] used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what [Vendor] has

done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action [Vendor] has taken or shall take to prevent future similar unauthorized use or disclosure. [Vendor] shall provide such other information, including a written report, as reasonably requested by School district.

5. [Vendor] shall report, either orally or in writing, to School district any use or disclosure of Covered Data not authorized by this Agreement or in writing by School district, including any reasonable belief that an unauthorized individual has accessed Covered Data. [Vendor] shall make the report to School district immediately upon discovery of the unauthorized disclosure, but in no event more than two (2) business days after [Vendor] reasonably believes there has been such unauthorized use or disclosure. [Vendor]'s report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the School district Covered Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what [Vendor] has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action [Vendor] has taken or shall take to prevent future similar unauthorized use or disclosure. [Vendor] shall provide such other information, including a written report, as reasonably requested by School district.

6. [Vendor] agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of [Vendor]'s security obligations or other event requiring notification under applicable law ("Notification Event"), [Vendor] agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the School district and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.

Protected Health Information (HIPAA)

Sample RFP Language:

1. Proposer may create, receive from or on behalf of School district, or have access to, records or record systems that are subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191). Describe the security features incorporated into the product to safeguard records subject to HIPAA.

2. Does the Proposer monitor the HIPAA Security Rule (45 C.F.R. § 164 subparts A, E (2002)) Required safeguards and the Proposer's own information security practices to ensure continued compliance? If yes, describe the Proposer's monitoring activities and their frequency.

Sample Contract Clauses:

1. HIPAA Compliance. [Vendor] agrees that it will execute a HIPAA Business Associate Agreement ("BAA") with School district and the BAA will be in the form set forth in Exhibit D, HIPAA Business Associate Agreement, attached and incorporated for all purposes.]

References to Third Party Compliance With District Policies, Standards, Guidelines, And Procedures

Sample RFP Language:

1. If the Proposer were to be selected, would the Proposer agree to comply with School district Information Security Policy? If Proposer objects to complying with School district policy, Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.

Sample Contract Clauses:

1. [Vendor] certifies that all systems and networking equipment that support, interact, or store School district data meet physical, Network and System security requirements as defined by the School district at (http:///) or that conform to the standards identified by the National Institute of Standards of Technology (NIST) https://csrc.nist.gov/publications/sp1800 where the School district's requirements control in the event of conflict. Significant deviation from these standards must be approved by the IT Manager. [Vendor] will notify the district within one (1) week if its systems and networking equipment do not conform to these requirements.

2. [Vendor] shall certify applications are fully functional and operate correctly as intended on systems using the U.S. Government Baseline Configurations The standard installation, operation, maintenance, update and/or patching of the software shall not alter the configuration settings, and applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

3. [Vendor] must comply with federal, state, and local laws concerning data privacy, as well as School district's data handling guidelines during the handling of School district data.

Security Audits and Scans (Independent Verification)

Sample RFP Language:

1. Has the Proposer undergone and would be willing to provide the results of a Statements for Standards for Attestation Engagement (SSAE 18) audit, or equivalent independent security audit, to attest to the strength of the Proposer's security practices and procedures? If Proposer objects to providing the audit results, Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.

2. If the Proposer were to be selected, would the Proposer agree to a vulnerability scan [penetration test performed by School district or a party of its choosing of all systems that would interact with the service proposed including any systems that would hold, process, or from which School district data may be accessed? If Proposer objects to the vulnerability scan [penetration test], Proposer must, as part of its proposal, identify and describe in detail the reasons for Proposer's objection.

Sample Contract Clauses:

1. [Vendor] agrees to have an independent third-party security audit performed at least once a year. The audit results and [Vendor]'s plan for addressing or resolving of the audit results shall be shared with the school district within XX (X) days of the [Vendor]'s receipt of the audit results. The audit should minimally check for buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other well-known vulnerabilities.

2. The school district reserves the right to require [Vendor] to provide the results of an audit of security policies, practices, and procedures on an annual or biennial basis. This audit must be performed by a third-party approved by the school district.

3. The school district reserves the right to request the results of a vulnerability scan for the [Vendor]'s production environment. Production environment is here defined as all systems that interact with the service contracted for herein including any systems that hold, process, or from which school district data may be accessed. A vulnerability scan is defined as a scan by a network vulnerability scanner such as Nessus or ISS.

4. The school district reserves the right to request the results of a formal penetration test. A penetration test is here defined as "the process of using approved, qualified personnel to conduct real-world attacks against a system so as to identify and correct security weaknesses before they are discovered and exploited by others."

Security Incident Investigations

Sample RFP Language:

1. What procedures and methodology does the Proposer have in place to manage security incidents including detection, notification, and investigation to mitigate any damage and to restore any lost School district data? [Include definition of security incident if it has not been defined in the RFP Definitions section already.]

Sample Contract Clauses:

1. In order to ensure the ability to investigate security incidents, [Vendor] agrees to retain all authentication logs for a minimum of three (3) months from the creation of such logs.

2. [Vendor] agrees to provide the school district with the name and contact information, including phone number and email address, of at least one security contact who will respond to the school district in a timely manner, dependent on criticality.

3. [Vendor] agrees to shut down ALL access to the school district's application on [Vendor]'s system within XX minutes notice from the school district's security representative.

4. Any product provided by [Vendor] must provide detailed logging of its transactions, including but not limited to: Privileged access to any sensitive information, including IP addresses of the user and original user name; Account creation, deletions, and modifications; Failed attempts to access data; All Logins (failed and successful) with IP address, using date, time, and user ID; Any OS patch or OS configuration changes and the user and IP address making them; Any changes to files in the web application directories, and the user and IP address making them; Any log file deleted and the user and IP address making the change; Any log file changed by the non-owing process and the user and IP address making the change; Service start/stop any service or server (i.e., any reboot of service or server outside of the normal maintenance window); and changes to firewall configuration files; and the user and IP address making the changes. Note, passwords should be excluded from all audit records, including records of successful or failed authentication attempts.

5. It is presumed that the consequences of a virus, Trojan, or worm infection; intrusion by unauthorized third parties; or similar security breaches are not beyond the control of [Vendor]." **Note:** Can be used as a qualifier of the Force Majeure clause.

Separate Document Addressing Data Protection

Sample RFP Language:

- Not Applicable. Best addressed with contract clauses.

Sample Contract Clauses:

1. If an School district intends to provide Confidential Digital Data to a third party acting as an agent of or otherwise on behalf of that School district (e.g., an application service provider) and if it determines that its provision of Confidential Digital Data to a third party will result in a significant risk to the confidentiality and integrity of such Data, a written agreement with the third party is required which must specify terms and conditions that protect the confidentiality and integrity of the Confidential Digital Data as required by this Policy. The written agreement must require the third party to use appropriate administrative, physical, and technical safeguards to protect the confidentiality and integrity of all Confidential Digital Data obtained and the School district, as applicable, should monitor compliance with the provisions of the written agreement.

State Breach Notification Laws

Sample RFP Language:

1. Describe the procedures and methodology in place to detect information security breaches and notify customers in a manner that meets the requirements of the state breach notification law.

Sample Contract Clauses:

1. [Vendor] agrees that it will execute a State Breach Notification Addendum with school district and the Addendum will be in the form set forth in Exhibit F, attached and incorporated for all purposes.

Student Education Records (FERPA)

Sample RFP Language:

1. Proposer may create, receive from or on behalf of School district, or have access to, records or record systems that are subject to the Family Educational Rights and Privacy Act ("**FERPA**"), 10 U.S.C. Section 1232g. Describe the security features incorporated into the product to safeguard FERPA records.

Sample Contract Clauses:

1. The [Vendor] acknowledges that certain information about the school district's students is contained in records maintained by the [Vendor] and that this information can be confidential by reason of the Family and Educational Rights and Privacy Act of 1974 (20 U.S. C. 1232g) and related School district policies currently at [insert applicable link [http://]] unless valid consent is obtained from the School districts' students or their legal guardians. Both parties agree to protect these records in accordance with FERPA and School district policy. To the extent permitted by law, nothing contained herein shall be construed as precluding either party from releasing such information to the other so that each can perform its respective responsibilities. The school district shall advise [Vendor] whenever any School district students have provided consent to release information to an extent broader than as provided for by FERPA or School district policy.

2. [Vendor] agrees that it may create, receive from or on behalf of School district, or have access to, records or record systems that are subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g (collectively, the "FERPA Records"). [Vendor] represents, warrants, and agrees that it will: (1) hold the FERPA Records in strict confidence and will not use or disclose the FERPA Records except as (a) permitted or required by this Agreement, (b) required by law, or (c) otherwise authorized by School district in writing; (2) safeguard the FERPA Records according

to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which [Vendor] protects its own confidential information; and (3) continually monitor its operations and take any action necessary to assure that the FERPA Records are safeguarded in accordance with the terms of this Agreement. At the request of School district, [Vendor] agrees to provide School district with a written summary of the procedures [Vendor] uses to safeguard the FERPA Records.

Use of Data

Sample RFP Language:

1. What administrative safeguards and best practices does the Proposer have in place to vet Proposer's and third-parties' staff members that would have access to the environment hosting all systems that would interact with the service proposed including any systems that would hold, process, or from which School district data may be accessed to ensure that School district data and resources will not be accessed or used in an unauthorized manner.

2. List all subcontractors that may have access to School district data and their corresponding location.

3. How will users authenticate to the proposed system? Does the proposed system allow for multiple security levels of access based on affiliation (e.g., staff, faculty, student), roles (e.g., system administrators, analysts, information consumers), and/or department? If yes, describe how the proposed system provides for multiple security levels of access.

4. Does the product provide the capability to limit user activity based on user type or role (i.e., who can create records, delete records, create and save reports, run reports only, etc.)? If yes, describe how the product provides that capability. If no, describe what alternative functionality is provided to ensure that users have need-to-know based access to the product?

5. What safeguards does the Proposer have in place to segregate School district data from system and other customers' data to prevent accidental and/or unauthorized access to School district data?

6. What safeguards does the Proposer have in place to prevent the unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of School district data?

Sample Contract Clauses:

1. The [Vendor] agrees that data provided to them during the provision of service shall be used only and exclusively to support the service and service execution and not for any other purpose. This shall include not examining data for targeted marketing either within the confines of the service or external to the service (e.g., keyword indexing). The [Vendor] may use aggregate statistics on service usage to enhance or optimize the functionality of the service. The phrase 'School district data' includes data uploaded by users of the service and communications between the user, the school district, and [Vendor].

2. Uses of School district data provided under this Agreement other than for the use as specifically detailed in this Agreement is strictly prohibited unless such other use is subsequently specifically agreed to in writing by the parties.

3. [Vendor] shall represent, warrant and certify it will: Not otherwise use or disclose Confidential Data except as required or permitted by law; Safeguard Confidential Data according to all commercially reasonable administrative, physical and technical standards (e.g., such standards established by the National Institute of Standards and Technology or the Center for Internet Security); Continually monitor its operations and take any action necessary to assure the Confidential Data is safeguarded in accordance with the terms of this Agreement.

4. Unless expressly permitted by the express advance written consent of an School district official authorized to give such consent, [Vendor] and its employees, agents, contractors, and other persons associated with [Vendor] (collectively, the "[Vendor] Users") are only permitted to use, reuse, distribute, transmit, manipulate, copy, modify, access, or disclose the school district data to the extent necessary for [Vendor] to implement and maintain the System as set forth in this Agreement. [Vendor] and the [Vendor] Users shall hold the school district data in confidence and protect the school district data to the same extent and in at least the same manner as [Vendor] protects its own data, but in no case in a lesser manner than a reasonable degree of care under the circumstances.

5. [Vendor] will be solely responsible for any unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of school district data and any non-compliance with the data privacy and security requirements by [Vendor] or [Vendor] users.

6. No school district Data may be outsourced or housed outside the United States of

[INSERT NAME OF EDUCATIONAL AGENCY]

and

[INSERT NAME OF CONTRACTOR]

This Data Privacy Agreement ("DPA") is by and between the [Insert name of Local Educational Agency] ("LEA"), an Local Educational Agency, and [Insert Name of Contractor] ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of private information including, Personally Identifiable Information(PII), Personal Health Information(PHI), Financial Information(FI), User Accounts & Passwords (USP), Annual Professional Performance Review(APPR) or student educational records in a manner not permitted by state and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to private information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of private information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of private information for advertising purposes; or the sale, use or disclosure of private information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of private information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Local Educational Agency**: A public board of education or other public authority legally constituted within a State for either administrative control or direction of, or to perform a service function for, public elementary schools or secondary schools in a city, county, township, school district, or other political subdivision of a State, or for a combination of school districts or counties that is recognized in a State as an administrative agency for its public elementary schools or secondary schools.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **Financial Information** Means identifiable information such as account numbers and routing numbers.
9. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
10. **Parent:** A parent, legal guardian or person in parental relation to the student.
11. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
12. **Private Information** Means Personally Identifiable Information, Private Health Information, Financial Information, and User Account Information.
13. **Protected Health Information** Protected Health Information is health information (i.e., a diagnosis, a test result, an x-ray, etc.) that is maintained in the same record set as individually identifiable information (i.e., a name, an address, a phone number, etc.).
14. **Release:** Shall have the same meaning as Disclose.
15. **School:** Any public elementary or secondary school authorized by the NJ Department of Education.
16. **Student:** Any person attending or seeking to enroll in an Local Educational Agency(LEA).
17. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
18. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
19. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.
20. **User Identification Information** Means user identification codes or passwords used to access computer or online systems.

ARTICLE II: PRIVACY AND SECURITY OF PRIVATE INFORMATION

1. **Compliance with Law.**
   In order for Contractor to provide certain services ("Services") to the LEA pursuant to a contract dated [Insert Date] ("Master Service Agreement"); Contractor may receive private information regulated by several New Jersey and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New Jersey Education Law Chapter 18A; and the New Jersey Administrative Code at 6, and 6A. The Parties enter this DPA to address the requirements of New Jersey law. Contractor agrees to maintain the confidentiality and security of private information in accordance with applicable New Jersey, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to private information, and Contractor must not use private information for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the way such Services are provided shall violate New Jersey law.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect private information in a manner that complies with New Jersey State, federal and local laws and regulations and the LEA's policies. The Contractor shall provide the LEA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **LEA's Data Security and Privacy Policy**
   The LEA has adopted a data security and privacy policy that aligns with the NIST Cyber Security Framework. Contractor shall comply with the LEA's data security and privacy policy and other applicable LEA policies.

5. **Right of Review and Audit.**
   Upon request by the LEA, Contractor shall provide the LEA with copies of its policies and related procedures that pertain to the protection of private information. It may be made

available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New Jersey State laws and regulations, the LEA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the LEA. Contractor may provide the LEA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors**.
   (a) Contractor shall only disclose private information to Contractor's employees and subcontractors who need to know the private information in order to provide the Services and the disclosure of private information shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
   (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to private information is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
   (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the LEA and remove such subcontractor's access to private information; and, as applicable, retrieve all private information received or stored by such subcontractor and/or ensure that private information has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises private information, Contractor shall follow the Data Breach reporting requirements set forth herein.
   (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
   (e) Contractor must not disclose private information to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the LEA of the court order or subpoena in advance of compliance but in any case, provides notice to the LEA no later than the time the private information is disclosed, unless such disclosure to the LEA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

Contactor shall ensure that all its employees and Subcontractors who have access to private information have received or will receive training on the federal and state laws governing data protection, data privacy, confidentiality of such data prior to receiving access. In addition, the contractor and any subcontractor will provide annual cybersecurity awareness training to all staff with access to LEA private information.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain private information or retain access to private information..

9. **Data Return and Destruction of Data**.

(a) Protecting private information from unauthorized access and disclosure is of the utmost importance to the LEA, and Contractor agrees that it is prohibited from retaining private information or continued access to private information or any copy, summary or extract of private information, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the LEA. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer private information, in a format agreed to by the Parties to the LEA.

(b) If applicable, once the transfer of private information has been accomplished in accordance with the LEA's written election to do so, Contractor agrees to return or destroy all private information when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all private information (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all private information maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that private information is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that private information cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the private information cannot be retrieved. Only the destruction of paper private information, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the LEA with a written certification of the secure deletion and/or destruction of private information held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. **Commercial or Marketing Use Prohibition.**
Contractor agrees that it will not sell private information or use or disclose private information for a Commercial or Marketing Purpose.

11. **Encryption.**
Contractor shall use industry standard security measures including encryption protocols that comply with New Jersey law and regulations to preserve and protect private information. Contractor must encrypt private information at rest and in transit in accordance with applicable New Jersey laws and regulations.

12. **Breach**.

(a) Contractor shall promptly notify the LEA of any Breach or incident related to private information without unreasonable delay no later than two (2) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach or incident which includes the date of the incident and the date of discovery; the types of private information affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the LEA. Notifications required by this section must be sent to the LEA's District Superintendent with a copy to the Information Technology Office. Violations of the requirement to notify the LEA shall be subject to a civil penalty. The Breach of certain private information protected may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the LEA at the following address:

[Name:

Title:

Address:

City, State, Zip:

Email:]

13. **Cooperation with Investigations.**
    Contractor agrees that it will cooperate with the LEA and law enforcement, where necessary, in any investigations into a Breach or Incident. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach or incident is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**
    Where a Breach of private information occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the LEA for the full cost of the LEA's notification to Parents, students, teachers, and staff.

15. **Notification of Breach or Data Security Incident to NJCCIC**
    NJ Cybersecurity and Communication Integration Cell is the state agency that needs to be notified in 72 hours of a breach or data incident related to LEA private information. The contractor shall provide the information requires by NJ Bill 297 or the New Jersey Identity Theft Protection Act to allow the district to file a timely notification to NJCCIC. If the contractor fails to provide the information, the contractor will be liable for any penalties assessed by NJCCIC.

16. **Termination**.
    The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all private information.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
    FERPA provide Parents and Students the right to inspect and review their child's or the Student Data stored or maintained by the LEA. To the extent any Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the LEA's requests for access to Student Data so the LEA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the LEA and refer the Parent or Eligible Student to the LEA.

2. **Bill of Rights for Data Privacy and Security**.
   The LEA has adopted the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**

   In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

   This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

LOCAL EDUCATIONAL AGENCY	**CONTRACTOR**
BY: ***[Signature]***	BY: ***[Signature]***
[Printed Name]	***[Printed Name]***
[Title]	**[Title]**
Date:	Date:

EXHIBIT A – Student's Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. Federal laws such as, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PRIVATE INFORMATION is stored or transferred.

5. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PRIVATE INFORMATION occurs.

6. Educational agency workers that handle PRIVATE INFORMATION will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

7. Educational agency contracts with vendors that receive PRIVATE INFORMATION will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	
[Title]	
Date:	

INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

The Local Educational Agency (LEA) should gather this information from the third-party contractors that will receive Private Information.

Name of Contractor	
Description of the purpose(s) for which Contractor will receive/access PII	
Type of PRIVATE INFORMATION that Contractor will receive/access	Check all that apply: ☐ Student PII ☐ Student PHI ☐ Student UI ☐ Student Records ☐ Parent PII ☐ Parent FI ☐ Parent UI ☐ Staff PII ☐ Staff PHI ☐ Staff FI ☐ Staff UI ☐ APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
Subcontractor Written Agreement Requirement	Contractor 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) ☐ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to LEA, or a successor contractor at the LEA's option and written discretion, in a format agreed to by the parties**.** • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PRIVATE INFORMATION will do so by contacting the EA. If a correction to data is deemed necessary, the LEA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the LEA's written request.

Secure Storage and Data Security	Please describe where private information will be stored and the protections taken to ensure private information will be protected: (check all that apply) ☐ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	
[Title]	
Date:	

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Local Educational Agency (LEA) should ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan. For every contract, the Contractor 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 the local educational agency data privacy and security policies in New Jersey**. Contractors should ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
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.	
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.	
5	Specify how you will manage any data security and privacy incidents that implicate PRIVATE INFORMATION 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 EA.	
6	Describe how data will be transitioned to the LEAwhen no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the LEA's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of	

Function	Category	Contractor Response
	unauthorized access to authorized activities and transactions.	
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	

Function	Category	Contractor Response
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	

<SCHOOL DISTRICT LOGO>

SOFTWARE/APP SUBSCRIPTION PURCHASE APPROVAL

Instructions: This form is for software titles whether installed or used through a web interface used at the teacher, class, building or district level. Building staff should complete, sections 1 through 4.

Section 1: Requestor Information			
Name of Person Making Request		Date	
Building		Email	
Room #		For Device #	

Section 2: Software/Subscription Information: ____ **Student Use** ____ **Staff Use** ____ **Student & Staff Use**			
Title:		Publisher:	
Type	Individual Class School District (Circle one)	Publisher Website	
Cost:		If Subscription Period	
Are student accounts required?		Do students need an email account to use software?	
Is student data stored in the System?	Yes - No	Is software being used with children < 13 years old?	

Section 3: Funding:

Budget Account(s): _____ Amount: $_____

Category	Presentation Mode	Feedback Mode	Student Progress Monitoring
__ Tutorial __ Drill & Practice __ Simulation __ Demonstration __ Reference __ Productivity __ Problem Solving __ Test __ Multimedia __ Other: Resource	__ Visual (Text) __ Visual (Images) __ Visual(Animation) __ Visual (Video) __ Auditory (Narrative) __ Auditory (Instructions) __ Auditory (Music) __ N/A	__ Visual (Text) __ Visual (Images) __ Auditory(Text) __ Auditory(Sound) __ Auditory(Music) __ N/A	__ Ongoing Feedback __ Autosave of Student Work __ Can Save Settings by Student __ Can Save Data for ____ Students __ Student Performance Report __ None

Section 4: Local Approvals:

Building Principal/Department Administrator: _____ Date: _____

<Technology Office> Approval Process:

Subscription/Software is - is not compatible with hardware in use at _____.

Publisher Terms of Service Reviewed: Yes No Date:_____ Policy is - is not compliant.

Link to Terms of Service: _____

Publisher Privacy Policy Reviewed: Yes No Date:_____ Policy is - is not compliant.

Link to Privacy Policy _____

Subscription/Software is - is not compliant with CIPA.

Subscription/Software is - is not compliant with COPPA.

Subscription/Software is - is not compliant with FERPA.

Subscription/Software is - is not compliant with PRAA.

Subscription/Software is - is not compliant with Student Records Policy

Approval:

____ Approved ____ Not Approved - Reason: _____

_____ Date: _____

<Technology Person/ School Business Administrator>

If Approved:

PO # _____ Date Entered:_____ Date Returned:_____

Third Party Vendor Data Protection Review Request Form

The use of external software solutions or service providers can result in risk for the school district. All protected information exposed through an external source is the legal responsibility of the district. To protect all parties, external technology relationships require contracts that manage these risks.

To ensure that appropriate information security considerations get integrated into the procurement process, all district schools and departments engaging in acquisitions of, or contracting for, information and instructional technology goods, software and services need to collaborate with:

- The Office of Information Technology to determine if the relationship risks require a contract. These risks can be access to personally identifiable information of students, employees or others resident in an external provider data system; and access to payroll information; and/or business office banking information if the external software can access district systems.
- The Business Office whenever service or transaction includes payment card information (PCI) and/or budget consideration.
- The Board Attorney, whenever existing vendor terms of service need Board Attorney review.

Information security related to software purchased or procured (freeware, open source) from third parties is to be evaluated prior to acquisition. This includes downloading of online tools (including plug-ins), SaaS (Software as a Service) subscriptions, and other software purchases made by accepting a click-through **e**nd **u**ser **l**icense **a**greement (EULA) and paid for by the District.

Federal or state regulations or contractual agreements may require additional actions that exceed those included above.

To facilitate a review, the request form below, along with relevant documents, should be completed and submitted to the District Office of Information Technology. The Office of Information Technology will respond within seven (7) business days after receipt of a completed vendor evaluation request. Requestors may be required to seek additional consultation with the Board Attorney or another department.

Third Party Vendor Data Protection Review Request Form

Submit this form to <vendormanagement@schooldomain.com> , for <Information Technology> to review.

School or department Requesting Review:	
Contact Name:	
Contact Title:	
Contact Email:	
Contact Phone:	
Date of Request:	

Vendor Name:	
Product Name:	
Product Type:	☐ Chrome App ☐ Android App ☐ IOS App ☐ Packaged Software ☐ Server Software ☐ Virtual Software ☐ Hosted Solution ☐ Hosted Software. ☐ Hosted Application ☐ Hosted Platform *Cloud Deployments:* ☐ Private Cloud ☐ Public Cloud. ☐ Hybrid Cloud ☐ Hosted Solution ☐ Hosted Application ☐ Hosted Platform *Cloud Services:* ☐ Software as a Service (SaaS) ☐ Infrastructure as a Service (IaaS) ☐ Platform as a Service (PaaS) ☐ Function as a Service (FaaS) ☐ Hardware Device ☐ IOT Sensors ☐ AAC Devices
Website:	
Contract Term:	State Date: End Date:
Purchase Method:	☐ Open Market ☐ Request for Proposal ☐ Quote ☐Bid ☐ Cooperative Pricing Coop:
Date Needed:	

Subcontractors	Contractor 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) ☐ Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Storage	Please describe where confidential and internal information will be stored, and the protections taken to ensure confidential and internal information will be protected: (check all that apply) ☐ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution. ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:
Encryption	

Briefly describe the product functionality and how your school or department plans to use it.			
Describe in detail what data the service will collect, process, or share.			
What is the sensitivity level of the data the service will collect, process, or share?			
_Public	_Internal	__Confidential	❑ Unsure

How widely will the service be used? (e.g., building/department-wide, district-wide, individual faculty/staff)
If requesting a data classification review, please STOP HERE. **If you are requesting a review of vendor documentation to get purchase approved, please continue with the rest of the form.**
Type of Data Vendor will receive or access: **PII- Personally Identifiable Information** **PHI- Personal Health Information** **PCI- Payment Card Data.** **APPR- Annual Professional Performance Review** **UID/PW- User ID & Password** **IEP: Individualized Education Program**
☐ Student PII ☐ Student PHI ☐ Student UID/PW ☐ Student IEP ☐ Parent PII ☐ Parent PHI ☐ Parent PCI/Financial Data ☐ Parent UID/PW ☐ Staff PII ☐ Staff PHI ☐ Staff PCI/Financial Data. ☐ Staff UID/PW ☐ Staff APPR ☐ Staff Biometric
Link to Vendor Terms of Service/Use
Link to Vendor Privacy Policy:
Link to Vendor Master Services Agreement:
Link to Vendor Security Policy:

Please submit pages 5 through 12 to the vendor to complete and provide the requested details to allow the <Information Technology Office> to complete its review.

#	Requirement	Meet Y/N	Description of the vendor's commitments to this requirement or link to requested information
2.1.1	Please describe what data your require for your service: personal information, financial information, confidential/sensitive data and government data		
2.1.2	Provide a data classification matrix including data definitions and access restrictions along with minimum controls for your service		
2.2.1	How do you encrypt customer data, please link relevant data.		
2.3.1	How does your organization decide who has access to district sensitive data ?		
2.3.2	Do you have the capabilities to anonymize data ?		
2.3.3	Which groups of staff and contractors have access to personal and sensitive data you handle ?		
2.3.4	Do you backup district data stored in your system?		
2.3.5	Do you test and document recovery of district data from these backups ?		
2.4.1	Do you have a password policy, does it have length and complexity requirements, do employees & contractors connecting to your production systems utilize multi-factor authentication?		
2.4.2	Do employees or contractors have the ability to connect remotely to your production system ?		

3.1.1	Do you have a documented information security program that includes administrative, technical, and physical safeguards?		
3.1.2	Is your information security program and policies reviewed annually ?		
3.2.1	Do you have an Information Security Risk Management Program?		
3.3.1	Do you have a dedicated information security team ?		
3.4.1	Are all employment candidate, contractors and involved third parties subject to background verification ?		
3.5.1	Are all employees and contractors require to sign an Acceptable Use Policy ?		
3.6.1	Are documented procedures followed when terminating an employee with access to district data verifying return of assets and revocation of access to your production systems ?		
4.1.1	How is your network security testing performed ? What is the frequency of testing ?		
4.2.1	How is your application security testing performed ? What is the frequency of testing?		
4.3.1	Summarize of attach your network vulnerability management process of procedures.		
4.3.2	What tools do you use for vulnerability management?		
4.3.3	What is the timeframe for you to patch critical vulnerabilities ?		
4.4.1	Are all endpoint devices connected to your production networks managed via an Endpoint Detection and Response System ?		
4.4.2	Describe standard device security		

	(Login Password, EDR/MDR, Encryption, Firewall, MFA etc)		
4.4.3	Do you limit data exfiltration to endpoint devices in your production environment ?		
4.5.1	Are all hosts where service of solution is running, uniformly configured?		
4.6.1	Are all security events logged ? Are logs reviewed?		
4.7.1	What encryption framework is used to secure data in transit over public networks ?		
4.7.2	What encryption framework is used to secure data at rest ?		
4.7.3	What encryption framework is used to secure and store passwords?		
4.7.4	How are encryption keys stored and managed within your system?		
4.8.1	Describe network security awareness training program for your personnel		
5.1.1	How do you keep aware of potential vulnerabilities and threats that may affect your service of solution?		
5.2.1	How do you log and alert relevant security threats ?		
5.3.1	Describe or attach your Incident Response Program ?		
5.3.2	How is your Incident Response Program tested, and what is the frequency?		
5.3.3	Do you have a formal service level agreement (SLA) for incident response ?		
5.3.4	Does the vendor agree to comply with applicable federal, state, and local laws and regulations regarding the storage, handling, and transmission of personally identifiable information?		

5.3.5	Does the vendor commit to providing notice to the district in the event of a suspected or actual breach or data security incident? How quickly will they notify us?		
5.3.5.1	Will the vendor be liable for costs and damages to the district associated with such a breach?		
5.3.5.2	Can the contract be terminated due to a breach?		
5.4.1	Does the vendor agree not to aggregate or de-identify district data without written consent?		
5.4.2	Does the vendor agree not to transmit district data outside the United States, or allow access to District Data from employees or contractors located outside the United States, without approval?		
5.5.1	Does the vendor agree not to disclose district data to other third-party suppliers or subcontractors without a signed confidentiality or non-disclosure agreement in place?		
5.6.1	Does the vendor agree to notify the district in writing if they are served with any subpoena, court order, or other legal request that calls for disclosure of district data?		
5.7.1	Does the vendor agree to return or destroy any district data, including archives and backups, upon request or at the end of the contract?		
5.8.1	Will the vendor provide the district documentation on the current state of its security program upon request, or allow the district to conduct a security assessment of the vendor?		
6.1.1	Does the vendor maintain cyber liability insurance with a minimum coverage of $1,000,000 per claim and $2,000,000 aggregate?		

SCHEDULE OF DATA
(TO BE COMPLETED BY VENDOR)

Please have contractor note, each type of information their system uses or collects:

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Student Observation data	
	Teacher Evaluation and Professional Growth Plan	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
	Staff attendance and absence data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred, or primary language)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Name	First and/or Last	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Third Party Vendor Data Protection Review Request Form

Category of Data	Elements	Check if used by your system
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low-income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Staff Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) [D number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Staff Identifiers	Local (School district) [D number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
Other	Other study work data – Please specify	

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data – Please specify	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

Please submit this form, along with any vendor-provided documentation or other documents for review, to <vendormanagement@schooldomain.com>

For <Office of Information Technology Use>

_____ Forwarded to Board Attorney for Contract Terms review.

_____ Approved Acquisition

_____ Denied Acquisition – Reason: _____

_____ _____

< Technology Manager Name> <Date>

Vendor Information

Vendor Name: Product Name:
Vendor Contact Name:
Vendor Contact Email:

Integration Detail

Which systems are you requesting to integrate with?

- ☐ <Student Information System>
- ☐ <Budget, Accounting, Payroll & Personnel>
- ☐ <Human Resources Management System>
- ☐ Other:

How will this product be integrated with the source systems?

- ☐ API
- ☐ Data Exports/Flat File Exchange

Fields to be Integrated

Table	Field	Rationale (How will this data be used)

1. VENDOR INFORMATION SECURITY ASSESSMENT

Provide and validate the information below

System Information

VENDOR Name:
Solution/System Name:
Service Model: (e.g., IaaS, PaaS, SaaS)
Fully Operational as of: Enter the date the system became fully operational.
Number of Customers (State/Others): Enter # of customers / # of other customers
Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or Other? If other, please describe.
System Functionality: Briefly describe the functionality of the system and service being provided.

1.1. Relationship to Other Vendors or CSPs

If this system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in tables below.

Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?				*If "yes," identify the underlying system.*

*List all **services** leveraged. The system from which the service is leveraged must be listed in Table 2-2 above.*

Leveraged Services

#	Service	Service Capability	System
1	*State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.*	*List the capability the service provides (e.g., load balancer, SIEM, database, audit logging).*	*Identify the system from which the service is being leveraged.*

1.2. Data Flow Diagrams

Insert Vendor-provided data flow diagram(s) and provide a written description of the data flows. The diagram(s) must:

- *clearly identify anywhere District data is to be processed, stored, or transmitted.*
- *clearly delineate how data comes into and out of the system boundary.*
- *clearly identify data flows for privileged, non-privileged and customer access; and*
- *depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.*

1.3. Separation Measures

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

1.4. System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is "yes," please briefly describe the connection. Also, if the answer to the last question is "yes," please complete Table 2-5 below.

System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?			
2	Does the system connect to a corporate or district infrastructure/network?			
3	Does the system connect to external systems?			*If "yes," complete table below.*

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type "None" in the first row.

Interconnection Security Agreements (ISAs)

		Does an ISA Exist?		
#	**External System Connection**	**Yes**	**No**	**Interconnection Description. If no ISA, please justify below.**
1				
2				

2. Capability Readiness

2.1. District Mandates

This section identifies district requirements applicable to all district approved systems. All requirements in this section must be met.

Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.

District Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Does the VENDOR utilize security boundary/threat protection devices to protect the network, system, application…e.g., firewalls intrusion detection/ prevention systems, end point protection etc.?		
2	Does the VENDOR can consistently remediate high risk vulnerabilities within 30 days and medium risk vulnerabilities within 60 days?		
3	Does the VENDOR and system meet N.J Open Public Records Act (OPRA) management requirements, including the ability to support record holds, and OPRA request requirements?		
4	Does the VENDOR store, process or transmit **district data** only in the continental US and is that data backed up in only US locations?		
5	Does the VENDOR have a process to securely dispose of district data from its systems upon request that is in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1 **and** will provide to the district a certificate of data destruction?		
6	All operating systems (OS) AND major application software components (e.g., Microsoft SQL, Apache Tomcat, Oracle Weblogic, etc.), must be up to date and not past, 1 version behind the most current release?		
7	Does the vendor have a current 3rd party attestation certification **and** is it regularly renewed? The district requires an independent 3rd party attestation (e.g., SOC 2 Type 2, or ISO 27001) ***prior to*** contract award for systems containing private data.		
8	Does the VENDOR's staff have appropriate background checks for unprivileged and privileged access and accounts according to Federal and/or district designation procedures for those systems that require it?		
9	Does the VENDOR encrypt all district data stored in their system while in transit, at rest? What type encryption is used: _____		
10	Does the VENDOR use transport layer security in their solution. Please note the version of TLS used: _____		

2.1.1. Identification and Authentication, Authorization, and Access Control

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated, and which sufficiently reduces the risk of impersonation?			
2	Does the system require multi-factor authentication (MFA) for privileged access accounts and functions?			
3	Is role-based access used, managed, and monitored?			
4	Does the system restrict non-privileged users from performing privileged functions?			
6	Does the system ensure secure separation of customer data?			
7	Does the system ensure secure separation of customer processing environments?			
8	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system?			.
9	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure?			
10	How will the district's password policy be enforced? District requires minimum 14-character complex passwords (Upper, Lower, Special Character & Numerical)			

2.1.2. Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software?			
2	Does the system store audit data in a tamper-resistant manner ?			
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions?			
4	Does the VENDOR log and monitor access to the system?			
5	Does the VENDOR have an Incident Response Plan(IRP) and a is that plan periodically tested or drilled?			
6	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track, and remediate security flaws?			*If the system contains no custom software development, do not answer Y or N. Instead, state "NO CUSTOM CODE" here.*
7	Does the VENDOR implement automated mechanisms for incident handling and reporting?			
8	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements?			
9	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? The State of NJ's requirement for security breach reporting is 72 hrs. of incident confirmation.			
10	If the VENDOR's solution provides email "send as" capabilities, does it support DMARC and DKIM for email protection?			*If the system does not support this feature, do not answer Y or N. Instead, state "Not Applicable" here.*

2.1.3. Contingency Planning and Disaster Recovery

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster?			
2	Does the system have alternate storage and processing facilities?			
3	Does the system have or use alternate telecommunications providers?			
4	Does the system have backup power generation or other redundancy?			
5	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers?			

2.1.4. Configuration and Risk Management

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system?			
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?			
3	Does the VENDOR follow a formal change control process that includes a security impact assessment?			
4	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes?			
5	Does the VENDOR prevent unauthorized changes to the system?			

6	Does the VENDOR perform **authenticated** operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable?			*Describe how the Vendor validated that vulnerability scans were fully authenticated.*
7	Does the VENDOR demonstrate the capability to remediate high risk vulnerabilities within 30 days and medium risk vulnerabilities within 60 days?			*Describe how the Vendor validated that the VENDOR remediates high vulnerabilities within 30 days and medium vulnerabilities within 60 days.*
8	When a high risk vulnerability is identified as part of continuous monitoring activities, does the VENDOR consistently check audit logs for evidence of exploitation?			

2.1.5. Data Center Security

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel?			
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records?			
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment?			

The Vendor must answer the questions below.

Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities?			

2.1.6. Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Vendor Dependencies and Agreements

#	Question	Yes	No	*Instructions*
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?			*If "yes," please complete table Vendor Dependencies below.*
2	Within the system, are all products still actively supported by their respective vendors?			*If any are not supported, answer, "No."*

#	Question	Yes	No	*Instructions*
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?			*If "yes," please complete table Formal Agreements Details below.*

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Vendor Dependency Details

			Still Supported?	
#	**Product and Vendor Name**	**Nature of Dependency**	**Yes**	**No**
1				
2				

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.

Formal Agreements Details

#	Organization Name	Nature of Agreement
1		
2		

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Organization's Security Representative or designee

_____

PLEASE PRINT NAME

_____ _____

SIGNATURE Date

SCHEDULE OF DATA
(To be completed by the Vendor)

Please have Vendor note, each type of information their system uses or collects:

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Student Observation data	
	Teacher Evaluation and Professional Growth Plan	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
	Staff attendance and absence data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred, or primary language)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Name	First and/or Last	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

SCHEDULE OF DATA
(To be completed by the Vendor)

Category of Data	Elements	Check if used by your system
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low-income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Staff Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) [D number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Staff Identifiers	Local (School district) [D number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
Other	Other study work data – Please specify	

SCHEDULE OF DATA
(To be completed by the Vendor)

Category of Data	Elements	Check if used by your system
Transcript	Student course grades	
	Student course data	
	Student course grades/performance scores	
	Other transcript data – Please specify	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored or collected by your application	