DATA PROTECTION ADDENDUM

THIS ADDENDUM is to be attached and be part of all purchase orders and contracts for all software, cloud-based applications, email services, document storage or other related internet-based or web-based tools including but not limited to Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS).

1. **Definitions.**

A. "Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

B. "District" means Loudoun County School Division.

C. "District Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by the District on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, and personnel data and metadata.

D. "End User" means the individuals authorized by the District to access and use the Services provided by the Vendor under this Agreement.

E. "Personally Identifiable Information" (or PII) includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in § 2.2-3801 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "health records" as defined in § 32.1127.1:03B of the Code of Virginia; "directory information" as defined by § 22.1-287.1 of the Code of Virginia; "medical information" as defined by § 32.1127.05A of the Code of Virginia "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal identification numbers such as passport, visa or state identity card numbers.

F. "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards of Technology (NIST) SP 800-88r1 guidelines relevant to data categorized as high security.

G. "Security Breach" means an event in which District Data is exposed to unauthorized disclosure, access, alternation, or use.

H. "Services" means any goods or services acquired by the District from the Vendor, including computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents via the Internet and used as part of the school activity.

I. "Vendor" means the firm or vendor selected by the District.

J. "Mining District Data" means to search through, access, or extract District Data, metadata, or information which is not necessary to accomplish the purpose(s) of this Agreement.

2. **Rights and License in and to District Data.** The parties agree that as between them, all rights including all intellectual property rights in and to District Data shall remain the exclusive property of the District, and Vendor has a limited, nonexclusive license as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give Vendor any rights, implied or otherwise, to District Data, content, or intellectual property, except as expressly stated in the Agreement.

3. **Intellectual Property Rights/Disclosure.**

A. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by Vendor as a work for hire (or its subcontractors) for the District will not be disclosed to any other person or entity.

B. Vendor warrants to the District that the District will own all rights, title and interest in any and all intellectual property created in the performance of this Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all district-created intellectual property created in the performance of this Agreement to the District, and will execute any future

assignments or other documents needed for the District to document, register, or otherwise perfect such rights.

C. Notwithstanding the foregoing, for grant collaboration pursuant to subcontracts under sponsored grants, intellectual property rights will be governed by the terms of the grant or contract to the District to the extent such grant or contract requires intellectual property terms to apply to subcontractors.

4. **Data Privacy.**

A. Vendor will use District Data only for the purpose of fulfilling its duties under this Agreement and will not share such data, including anonymized data, with or disclose it to any third party without the prior written consent of the District, except as required by law.

B. District Data will not be stored or processed outside the United States without prior written consent from the District.

C. Vendor will provide access to District Data, including anonymized only to its employees and subcontractors who need to access the data to fulfill Vendor obligations under this Agreement. Vendor will ensure that employees and subcontractors who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement. If Vendor will have access to "education records" for the District's students as defined under the Family Educational Rights and Privacy Act (FERPA), the Vendor acknowledges that for the purpose of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the District Education records, as those terms have been defined under FERPA and its implementing regulations, and the Vendor agrees to abide by the FERPA limitations and requirements imposed on school officials. Vendor will use the Education records only for the purpose of fulfilling its duties under this Agreement for District's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the District.

D. Vendor will not use District Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by this agreement or otherwise authorized in writing by the District.

E. Vendor agrees to assist District in maintaining the privacy of District's Data as may be required by State and Federal law, including but not limited to the Protection of Pupil Rights Amendment (PRRA), The Children's Online Privacy Protection Act (COPPA), and the Government Data Collection and Dissemination Practices Act of Virginia.

DATA PROTECTION ADDENDUM

5. **Data Security.**

A. Vendor will store and process District Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all electronic District Data will be encrypted in transmission using, at minimum, Transport Layer Security (TLS) 1.2 (including via web interface) and stored at no less than 256-bit level encryption.

B. Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement.

6. **Employee and Subcontractor Qualifications.**

A. Vendor shall ensure that its employees and subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this agreement including but not limited to all terms relating to data and intellectual property protection.

B. If the Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of District Data known as Personally Identifiable Information or financial or business data which has been identified to the Vendor as having the potential to affect the accuracy of the District's financial statements, Vendor shall perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act Social Security Number trace; Social Security Number Death Master Search (SSNDMS);seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC); Criminal Records 7 Year Upper Court Search; and Multi State Sex Offender Registry Search.

7. **Data Authenticity and Integrity.** Vendor will take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity. Vendor shall be responsible for ensuring that District Data is retrievable in a format that can be easily read in compliance with the General Schedules of the Library

of Virginia, but not limited to, General Schedules 02,19 and 21 of the Library of Virginia in accordance with § 42.1-85, of the Code of Virginia.

8. **Security Breach.**

A. Response. Immediately upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of District Data, Vendor, will notify the District, in accordance with Section 18 of this Addendum, to fully investigate the incident, cooperate fully with the District's Investigation, and provide timely response to the incident. Except as otherwise required by law, Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the District.

B. Liability. In addition to any other remedies available to the District under law or equity, Vendor will reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused in whole or in part by Vendor or subcontractors, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the District as a result of the Security Breach.

9. **Response to Legal Orders, Demands or Requests for Data.**

A. Except as otherwise expressly prohibited by law, Vendor will:

(1) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data;

(2) consult with the District regarding its response;

(3) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and

(4) upon the District's request, provide the District with a copy of its response.

B. If the District receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act)

("requests") or request seeking District Data maintained by Vendor, the District will promptly provide a copy of the request to Vendor. Vendor will promptly supply the District with copies of records or information required for the District to respond, and will cooperate with the District's reasonable requests in connection with its response.

10. **Data Transfer Upon Termination or Expiration.**

A. Upon termination or expiration of this Agreement, Vendor will ensure that all District Data are securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within a responsible period of time, and without significant interruption in service. Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. In the event that the District requests destruction of its data, Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Vendor might have transferred District data. The Vendor agrees to provide documentation of data destruction to the District.

B. Vendor will notify the District of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the District access to Vendor's facilities to remove and destroy District-owned assets and data. Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the District. Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the District. Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the District, all such work to be coordinated and performed in advance of the formal, transition date.

11. **Audits.**

A. The District reserves the right in its sole discretion to perform audits of Vendor at the District's expense to ensure compliance with the terms of this Addendum. The Vendor shall reasonably cooperate in the performance of such audits. This provision applied to all agreements under which the Vendor must create, obtain, transmit, use, maintain, process, or dispose of District Data.

B. If the Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of District Data known as Personally Identifiable Information or financial or business data which has been identified to the Vendor as having the potential to affect the accuracy of the District's financial statements, Vendor will at District's expense conduct or have conducted at least annually:

(1) American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objective deemed sufficient by the District, which attests the Vendor's security policies, procedures and controls;

(2) vulnerability scan, performed by a scanner approved by the District, of Vendor's electronic systems and facilities that are used in any way to deliver electronic service under this Agreement; and

(3) formal penetration test, performed by a process and qualified personnel approved by the District, of Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement.

Additionally, the Vendor will provide the District upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement. The District may require, at District expense, the Vendor to perform additional audits and tests, the results of which will be provided promptly to the District.

12. **Institutional Branding.** Each party shall have the right to use the other party's Brand Features only in connection with performing the functions provided in this Addendum. Any use of a party's Brand Features will inure to the benefit of the party holding intellectual property rights in and to those features.

13. **Compliance.**

A. Vendor will comply with all applicable laws and industry standards in performing services under this Agreement. Any Vendor personnel visiting the District's facilities will comply with all applicable District policies regarding access to, use of, and conduct within such facilities. The District will provide copies of such policies to Vendor upon request.

B. Vendor warrants that any subcontractors used by Vendor to fulfill its obligations under this agreement will be subject to and will comply with each and every term

of this Data Protection Addendum in the same manner that Vendor itself is subject to the terms of this Data Protection Addendum.

C. Vendor warrants that the service it will provide to the District is fully compliant with and will enable the District to be in compliance with relevant requirements of all laws, regulation, and guidance applicable to the District and/or Vendor, including but not limited to: Student Privacy Pledge, the Children's Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act. (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Protection of Pupil Rights Amendment (PPRA); Americans with Disabilities Act (ADA), and Federal Export Administration Regulations.

14. **Conflict Other Agreements Between the Parties.** If there is any conflict or potential conflict between the terms of this Data Protection Addendum and the terms of any other agreements between the parties, the terms of this Data Protection Addendum shall control.

15. **No End User Agreements.** This Agreement is the entire agreement between the District (including District employees and other End Users) and the Vendor. In the event that the Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with District employees or other End Users, such agreements shall be null, void and without effect, and the terms of this Agreement shall apply.

16. **Terms and Terminations.**

A. Term. This Addendum will become effective when the Vendor accepts the Purchasing Terms and Conditions and is issued a Purchase Order for goods or services or receives payment by purchase card or check which necessitate that the Vendor create, obtain, transmit, use, maintain, process, or dispose of District Data in order to fulfill its obligations to the District. It will continue in effect until all obligations of the Parties have been met, unless terminated as provided in this section. In addition, certain provisions and requirements of this Addendum will survive its expiration or other termination in accordance with Section 15 herein.

B. Termination by the District. The District may immediately terminate the Agreement if the District makes the determination that the Vendor has breached a material term of this Data Protection Addendum.

C. Automatic Termination. This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement between the Parties.

17. **Survival.** The Vendor's obligations under Section 10 shall survive termination of this Agreement until all District Data has been returned or Securely Destroyed.

18. **Notices.** Any notices to be given will be made via certified mail or express courier to the address given below, except that notice of a Security Breach shall also be given as provided in Section 8.A. of this Addendum.

If to the Vendor:

COMPANY NAME, CONTACT NAME, and ADDRESS as listed on the Purchase Order

If to the District:

Mrs. Andrea Philyaw
Procurement Director
Loudoun County Public Schools
21000 Education Court
Ashburn, Virginia 20148
Telephone: 571-252-1270

With a copy to:

Stephen L. DeVita, Esquire
Division Counsel
Loudoun County Public Schools
21000 Education Court
Ashburn, Virginia 20148
Telephone: 571-252-1000; Facsimile: 571-252-1003

If notice concerns a Security Breach:

Dr. Rich Contartesi
Assistant Superintendent of Technology Services
Loudoun County Public Schools
21000 Education Court
Ashburn, Virginia 20148
Telephone: 571-252-1000

19. **Advertisement.** Any and all forms of advertisement, directed towards children, parents, guardians or District employees, as a result of this Agreement, shall be strictly prohibited.

20. **Governing Law.** This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Virginia, excluding its choice of law rules. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the Circuit Court for Loudoun County, Virginia.

SO AGREED:

LOUDOUN COUNTY SCHOOL BOARD	VENDOR
BY:_____	BY:_____
Title: _____	Title: _____
Date: _____	Date: _____