DATA PROTECTION ADDENDUM

BETWEEN: Fauquier County Public Schools ("District") and

Vendor name/address:	ExploreLearning, LLC 110 Avon Street, Suite 300 Charlottesville, VA 22902
Goods/Service:	ExploreLearning Reflex

This Data Protection Addendum ("Addendum") is to be attached and be part of all purchase orders and contracts where the Vendor provides goods or services which necessitate that the Vendor create, obtain, transmit, use, maintain, process, or dispose of District Data (as defined in the Definitions section (Exhibit "A") of this Addendum) in order to fulfill its obligations to the District. Given the critical nature of Student Data and Information, this Addendum, once fully executed, shall be incorporated into and become part of the Service Agreement, even if not specifically referenced in that Service Agreement.

The purpose of this Addendum is to describe the duties and responsibilities to protect student data transmitted to Provider from the District pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including but not limited to the FERPA, PPRA, COPPA, HIPPA, and the Code of Virginia § 22.1-289.01.

Requested changes to this Addendum are described in Exhibit "D".

1. **Nature of Services Provided**. The Vendor has agreed to provide the following digital educational services described as outlined in Exhibit "B" hereto:

2. **Data to Be Provided**. In order to perform the Services described in the Service Agreement, District shall provide the categories of data described as indicated in the Schedule of Data, attached hereto as Exhibit "C".

3. **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.

   3.1. **Use of De-identified Data.** Vendor may use De-identified Data for purposes of research, the improvement of Vendor's products and services, and/or the development of new products and services. In no event shall Vendor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

4. **Intellectual Property Rights/Disclosure**.

   4.1. 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 (or its subcontractors) for the District will not be disclosed to any other person or entity.

   4.2. Vendor warrants to the District that the District will own all rights, title and interest in any and all intellectual property created by students or staff 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.

   4.3. 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.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.

6. **Parent Access**. Provider and the District shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the District's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the District, who will follow the necessary and proper procedures regarding the requested information.

7. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the District. Provider shall notify the District in advance of a compelled disclosure to a Third Party unless legally prohibited.

8. **Data Privacy**.

   8.1. Vendor shall 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.

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

8.3. Vendor shall 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 shall 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 shall 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 **may** be designated as, and acting in the capacity of, 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 shall 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.

8.4. Vendor shall 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.

8.5. 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.

9. **Data Security**.

9.1. Vendor shall 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 SSL (Secure Sockets Layer) (including via web interface) and stored at no less than 128-bit level encryption.

9.2. Vendor shall 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.

10. **Employee and Subcontractor Qualifications**.

10.1. Vendor shall ensure that its employees and subcontractors who have 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 Addendum including but not limited to all terms relating to data and intellectual property protection.

10.2. 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; 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).The District reserves the right to request verification that the Vendor has performed the required background checks.

11. **Data Authenticity and Integrity**. Vendor shall 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.

12. **Security Breach**.

12.1. **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 shall notify the District in accordance with Section 22, fully investigate the incident, and cooperate fully with the District's Investigation of and response to the incident. Vendor shall follow the following process:

12.1.1. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", and "For More Information". Additional information may be provided as a supplement to the notice.

12.1.2. The security breach notification described above in section 12.1.1 shall include, at a minimum, the following information:

12.1.2.1. The name and contact information of the reporting District subject to this section.

12.1.2.2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

12.1.2.3. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

12.1.2.4. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

12.1.2.5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

12.1.3. At District's discretion, the security breach notification may also include any of the following:

12.1.3.1. Information about what the agency has done to protect individuals whose information has been breached.

12.1.3.2. Advice on steps that the person whose information has been breached may take to protect himself or herself.

12.1.4. Except as otherwise required by law, Vendor shall 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.

12.2. **Liability.** In addition to any other remedies available to the District under law or equity, Vendor shall 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.

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

13.1. Except as otherwise expressly prohibited by law, Vendor shall:

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

13.1.2. consult with the District regarding its response;

13.1.3. 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

13.1.4. upon the District's request, provide the District with a copy of its response.

13.2. 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 shall 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.

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

14.1. Upon termination or expiration of this Agreement, Vendor shall 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 30 days, 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.

14.2. Vendor shall 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 shall 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 shall 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.

15. **Audits**.

15.1. 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 Agreement. 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.

15.2. 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 at its expense conduct or have conducted at least annually:

(1) American Institute of CPSs 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.

15.3. The Vendor shall 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.

16. **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 Agreement. 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.

17. **Compliance**.
    17.1. Vendor shall 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

    17.2. 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.

    17.3. 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: 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.

18. **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.

19. **No End User Agreements**. 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, the District may request that such agreements shall be null, void and without effect, and the terms of this Agreement shall apply.

20. **Terms and Terminations**.

    20.1. **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 20 herein.

20.2. **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.

20.3. **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.

21. **Survival**. The Vendor's obligations under Section 14 shall survive termination of this Agreement until all District data has been returned or securely destroyed.

22. **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 12 of this Addendum.

22.1. If to the Vendor:

ExploreLearning, LLC
Joselyn Whetzel
110 Avon Street, Suite 300
Charlottesville, VA 22092
Telephone: 866-882-4141
Email: sales@explorelearning.com

22.2. If to the District:

Louis McDonald, Director of Technology
Fauquier County Public Schools
320 Hospital Drive, Suite 40
Warrenton, VA 20186
Telephone: 540-422-7013
Email: Louis.McDonald@fcps1.org

22.3. With a copy to:

Susan Monaco, Procurement Manager
Fauquier County Govt/Public Schools Procurement Div.
320 Hospital Drive, Suite 23
Warrenton, VA 20186
Telephone: 540-422-8348
Email: Susan.Monaco@fauquiercounty.gov

22.4. If notice concerns a Security Breach:

Louis McDonald
Director of Technology Services
Fauquier County Public Schools
320 Hospital Drive, Suite 40
Warrenton, VA 20186

Telephone: 540-422-7013
Email: Louis.McDonald@fcps1.org

23. **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.

24. **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 Fauquier County, Virginia.

25. **Indemnification**. Vendor shall indemnify, defend and hold harmless District and District's affiliates, officers, directors, and employees from and against any third-party claims, demands, causes of action, judgments, damages, liabilities, costs and expenses (including reasonable attorney's fees) arising from or relating to Vendor's or any of Vendor's employees, agents, contractors, or representatives unauthorized use, misuse, or illegal use of District Information or De-identified Information or any breach of this Agreement by Vendor. The District and any indemnified party shall cooperate and comply with the reasonable requests of Vendor in connection with the defense of any such claim. The receipt or providing such assistance is not a waiver of any alleged breach nor does the acceptance of such assistance constitute a waiver of any such breach by the District. Vendor shall control the defense and settlement of any such claim.

SO AGREED:

FAUQUIER COUNTY PUBLIC SCHOOL BOARD		EXPLORELEARNING, LLC	
BY:	Susan Monaco	BY:	David Shuster, Ph.D.
Title:	FCPS Procurement Manager	Title:	Founder/President
Date:	8/23/18	Date:	13 August 2018
Signature:	Susan Monaco	Signature:	

EXHIBIT "A"

DEFINITIONS

a. "**Agreement, Service or otherwise**" means any contractually binding document signed by the Vendor and the District legally obligating both parties; also referred to as "Contract", "Software Agreement", "Purchase Agreement".

b. "**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.

c. "**District**" means Fauquier County Public School Division.

d. "**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.

e. "**Elementary and secondary school purposes**" means purposes that (i) customarily take place at the direction of an elementary or secondary school, elementary or secondary school teacher, or school division; (ii) aid in the administration of school activities, including instruction in the classroom or at home; administrative activities; and collaboration between students, school personnel, or parents; or (iii) are otherwise for the use and benefit of an elementary or secondary school.

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

g. "**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 § 32.1- 127.1:03B of the Code of Virginia; "directory information" as defined by § 22.1-287.1 of the Code of Virginia; "medical information" as defined by § 32.1-127.05A 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.

h. "**Personal profile**" does not include account information that is collected and retained by a school service provider and remains under control of a student, parent, or elementary or secondary school.

i. "**School-affiliated entity**" means any private entity that provides support to a local school division or a public elementary or secondary school in the Commonwealth. "School-affiliated entity" includes alumni associations, booster clubs, parent-teacher associations, parent-teacher-student associations, parent-teacher organizations, public education foundations, public education funds, and scholarship organizations.

j. "**School service**" means a website, mobile application, or online service that (i) is designed and marketed primarily for use in elementary or secondary schools; (ii) is used (a) at the direction of teachers or other employees at elementary or secondary schools or (b) by any school-affiliated entity; and (iii) collects and maintains, uses, or shares student personal information. "School service" does not include a website, mobile application, or online service that is (a) used for the purposes of college and career readiness assessment or (b) designed and marketed for use by individuals or entities generally, even if it is also marketed for use in elementary or secondary schools.

k. "**School service provider**" means an entity that operates a school service pursuant to a contract with a local school division in the Commonwealth.

l. "**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 800-88 guidelines relevant to data categorized as high security.

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

n. "**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.

o. "**Student personal information**" means information collected through a school service that identifies a currently or formerly enrolled individual student or is linked to information that identifies a currently or formerly enrolled individual student.

p. "**Targeted advertising**" means advertising that is presented to a student and selected on the basis of information obtained or inferred over time from such student's online behavior, use of applications, or sharing of student personal information. "Targeted advertising" does not include advertising (i) that is presented to a student at an online location (a) on the basis of such student's online behavior, use of applications, or sharing of student personal information during his current visit to that online location or (b) in response to that student's request for information or feedback and (ii) for which a student's online activities or requests are not retained over time for the purpose of subsequent advertising.

EXHIBIT "B"

DESCRIPTION OF SERVICES
(TO BE COMPLETED BY VENDOR)

VENDOR NAME: ExploreLearning, LLC

ExploreLearning Reflex is adaptive and individualized, Reflex is the most effective system for mastering basic facts in addition, subtraction, multiplication and division for grades 2+.

Full of games that students love, Reflex takes students at every level and helps them quickly gain math fact fluency and confidence. Both educators and parents love the powerful reporting that allows them to monitor progress and celebrate success.

EXHIBIT "C"

SCHEDULE OF DATA
(TO BE COMPLETED BY VENDOR)

In order to perform the services described in Exhibit B, the vendor shall provide (check) the categories of data described below

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	x
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	x
Assessment	Standardized test scores	
	Observation data	x
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	x
	Ethnicity or race	x
	Language information (native, preferred or primary language spoken by student)	x
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	x
	Student grade level	x
	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	x
	Phone	

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	x
	Low income status	x
	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	
Student Identifiers	Local (School district) ID number	x
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	x
	Student app passwords	x
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)	x
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	

EXHIBIT "D"

AMENDMENT TO DATA PROTECTION ADDENDUM
(TO BE COMPLETED BY VENDOR)

If there are changes to the Data Protection Addendum, please describe the changes by providing the original language and requested change.

Original Language	Page Number	Requested Change
12.1. 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 shall notify the District in accordance with Section 22, fully investigate the incident, and cooperate fully with the District's Investigation of and response to the incident. Vendor shall follow the following process:	4	12.1. Response. Promptly 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 shall notify the District in accordance with Section 22, fully investigate the incident, and cooperate fully with the District's Investigation of and response to the incident. Vendor shall follow the following process:
13.1.1. immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data;	5	13.1.1. Promptly notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data;
14.1. Upon termination or expiration of this Agreement, Vendor shall ensure that all District Data are securely retumed or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within 30 days, and without significant interruption in service.	5	14.1. Upon termination or expiration of this Agreement, Vendor shall ensure that all District Data are securely retumed or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within 60days, and without significant interruption in service.
19. No End User Agreements. 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, the District may request that such agreements shall be null, void and without effect, and the terms of this Agreement shall apply.	7	19. No End User Agreements. 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, the District may request that such agreements, , to the extent they conflict with the terms of this Agreement, shall be null, void and without effect, and the terms of this Agreement shall apply.

May it be known that the undersigned parties, for good consideration, do hereby agree to make the following changes and / or additions that are outlined above. These additions shall be made valid as if they are included in the original stated Data Protection Addendum. No other terms or conditions of the Data Protection Addendum shall be negated or changed as a result of this here stated addendum.

SO AGREED:

FAUQUIER COUNTY PUBLIC SCHOOL BOARD		EXPLORELEARNING, LLC	
BY:	Susan Monaco	BY:	David Shuster, Ph.D.
Title:	FCPS Procurement Manager	Title:	Founder/President
Date:	8/23/18	Date:	13 August 2018
Signature:	Susan Monaco	Signature:	