ADDENDUM NO. 7

July 6, 2023

RE: **Bid #116.23.B6,** RFP – Cloud Based Adapted Reading Program

FROM: **Purchasing Office**
Howard County Public Schools
10910 Clarksville Pike
Ellicott City, MD 21042
(410) 313-6723
(410) 313-6789 fax

TO: APPROVED PROSPECTIVE BIDDERS

This addendum forms a part of the Contract Documents and modifies the Original Bidding Documents as noted below. Acknowledge receipt of this Addendum in the space provided on the Bid Price Sheet/Form of Proposal. Failure to do so may subject the Bidder to disqualification. This Addendum consists of three (3) pages.

A. Questions and Answers

1. .Appendix B, Definition of "Client Data," Page 42; Appendix B, Section E, Data De-Identification, Page 42: Contractor wishes to clarify that, for the purposes of the RFP and any potential agreement between the parties, Client Data does not include de-identified data, which refers to data generated from usage of Contractor's software from which all personally identifiable information has been removed or obscured so that it does not identify any individual and there is no reasonable basis to believe that the information can be used to identify any individual. Contractor utilizes trusted third-party providers to conduct research using de-identified data to improve its products. Such research is allowable under FERPA, and such third-party providers sign agreements with Contractor prohibiting attempts to re[1]identify de-identified data.

Response: HCPSS accepts this exception.

2. Appendix B, Section N(2), Page 44: Contractor wishes to clarify that, due to the inherent risks associated with the products being purchased under this RFP, Contractor shall remediate any high-level security vulnerabilities in a timely manner. 13. Appendix B, Section P, Employee and Subcontractor Qualifications, Pages 44-45: Contractor wishes to clarify that all employees and subcontractors with access to Client Data are required to receive FERPA training.

Response: HCPSS agrees.

3. Data Protection and Controls. B. 2 While LEXIA follows many industry best practices to reduce the systems' surface of vulnerability, it does not currently test for alignment with Center

for Internet Security (CIS) guide and therefore does not certify to full alignment with the CIS guide.

Response: HCPSS not accept this exception.

4. Data Protection and Controls. B. 7 The aforementioned section is modified to reflect the following: Lexia enables appropriate logging parameters to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards and as informed by ISO 27001

Response: HCPSS does not accept this exception.

5. Data Protection and Controls. B. 8 Per Lexia's internal policies, Lexia does not provide to external parties the aforementioned procedures. As such, the aforementioned section is modified to reflect the following: HCPSS shall have the right to inspect these policies and the Contractor or subcontractor's performance to confirm the effectiveness of these measures for the services being provided under the Contract.

Response: HCPSS does not accept this exception.

6. Data Protection and Controls. B. 12 Lexia does not annually review the aforementioned requirement.

Response: HCPSS does not accept this exception.

7. Data Protection and Controls. B. 13 Lexia applications undergo an almost annual penetration testing. Any Vulnerabilities that are identified are then patched and evaluated with internal risk assessment standard and protocols. Per Lexia's internal policies, Lexia does not provide to external parties the aforementioned procedures. As such, the aforementioned section is modified to reflect the following: HCPSS shall have the right to inspect the Contractor's policies and the results of vulnerability testing to confirm the effectiveness of these measures for the services being provided under the Contract

Response: HCPSS does not accept this exception.

8. Data Protection and Controls. B. 14 Lexia has its own standards, as identified in the bid submission. The County may also elect to utilize a sign onto single sign on option that adheres to District's own standard.

Response: HCPSS does not accept this exception.

9. Data Protection and Controls. B. 15 The policy on portable devices in the aforementioned section is modified to reflect the following: Lexia has in place tools, policies or protocols to protect student data stored on personnel's laptop or mobile electronic devices. At a minimum, Lexia will obtain a service that will allow Lexia to remotely wipe the hard drive on stolen laptops, remove access to authorized applications on mobile electronic devices, and locks for all

laptops and mobile electronic devices. Lexia also represents and warrants that if County data is to be stored on a laptop or other mobile electronic device, that such electronic devices are encrypted. Upon termination or completion of the contract, Lexia will ensure that the County Data has been securely deleted and destroyed in accordance with applicable law and Lexia's internal policies. Additionally, upon termination of any employee or agent all laptops will be scanned to ensure that no County Data is stored on such electronic devices. Further, upon termination of any employee or agent all access to authorized mobile device applications will be removed to ensure that no County Data is accessed through such mobile device applications.

Response: HCPSS does not accept this exception.

10. Data Protection and Controls. B. 18 Per Lexia's internal policies, Lexia does not provide to external parties the aforementioned procedures. As such, the aforementioned section is modified to reflect the following: HCPSS shall have the right to inspect these policies and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under the Contract.

Response: HCPSS does not accept this exception.

12.) Security Plan (A) The aforementioned section is modified to reflect the following: The Contractor shall protect HCPSS data according to a written security policy ("Security Plan") as informed Iso 27001 and shall supply a copy of such policy to HCPSS for validation, with any appropriate updates, upon written request.

Response: HCPSS does not accept this exception.

11. Data Protection and Controls. B. 17 Lexia does not confirm alignment with the aforementioned section. Lexia addresses the concerns in the aforementioned section through internal controls such as quarterly OS patching, limiting the lifecycle of the machines, and running anomaly detection across the server.

Response: HCPSS does not accept this exception.

12. SOC 2 Audit Report Lexia does not currently have a SOC 2 Type 2 audit and does not have a SOC 2 Type 2 audit on its road map for the current contracting year or in the future. Lexia has elected to undergo and adhere to the ISO-27001 audit. Lexia currently has a ISO27001 audit. The aforementioned section shall be modified to reflect the aforementioned Lexia election.

Response: HCPSS does not accept this exception.

13. While audits are permissible, during the audit process we will not provide information that would put the confidentiality of any other customer at risk.

Response: HCPSS accepts this.