DocuSign Envelope ID: 2E0ACFB0-EF21-4677-8FB4-7FE98E120CE1

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT

BETWEEN

ERIE 1 BOCES AND [*EVERFI*]

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with [*EVERFI*] which governs the availability to Participating Educational Agencies of the following Product(s):

EVERFI's K-12 Digital Resources

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with [*EVERFI]* which governs the availability to Participating Educational Agencies of the following Product(s):

EVERFI's K-12 Digital Resources

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Notwithstanding anything to the contrary herein, the parties agree that EverFi may, in accordance with its General Privacy Policy (https://everfi.com/privacy-policy/), provide de-

identified data to third party sponsors who provide funding for courses to assess learning progress of users as well as provide further educational opportunities.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will attempt to ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

Blackbaud maintains a robust cyber security awareness program in line with industry best practice. Every Blackbaud employee goes through a general Information Security Awareness training upon hire, and every year after. All employees are trained during annual information security awareness training on how to report security incidents, phishing, and suspected privacy incidents. Additional targeted training is provided to these employees based on their particular job functions, which could be in the form of peer training, traditional face-to-face training by a contracted professional, through conferences, computer-based training, and more. Blackbaud conducts organization-wide Security Awareness training on a regular basis. Additionally, developers are all trained annually on secure code techniques and OWASP Top Ten.

Upon hire and annually as part of the Cyber Security Awareness training, every Blackbaud/EverFi employee must agree in writing to appropriate security and confidentiality requirements.

Duration of MLSA and Protected Data Upon Expiration:

The MLSA commences on July 1, 2024 and expires on June 30, 2027.

Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

wnyric www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892
erie boces

In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.

Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.