

Addendum B

Supplemental Information Addendum

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by Education Analytics (EA) (the "Service Provider") are limited to the purposes authorized in the Agreement for Scheduled Services between the Vendor and the Fallsburg Central School District (the "Client") (the "Agreement") from 3/01/2023 until 12/31/2023.
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Service Provider will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"), Education Law 2-d; 8 NYCRR Part 121).
3. **CONTRACT PRACTICES:** The Agreement commences and expires on the dates set forth in the Agreement, unless earlier terminated or renewed pursuant to the terms of the Agreement. Protected data will be destroyed by the Service Provider within one (1) year after it is no longer needed to perform the institutional functions described in the Agreement, or upon termination of the Agreement, whichever occurs first or unless otherwise agreed to in writing by the Parties.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the Client in Service Provider's product and/or service by following the Client's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by Client in Service Provider's product and/or service by following the appeal procedure in the Client's APPR Plan. Unless otherwise required by the above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Service Provider by the Client will be stored in electronic memory (on servers or other computers) operated and maintained by or on behalf of Service Provider in the United States. The measures that Service Provider takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Service Provider will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.