EXHIBIT A: New York Ed Law 2-d DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including Parental Bill of Rights for Data Security and Privacy And Supplemental Information about a Master Services Agreement between School or District and Diffit, Inc.

1. Purpose

(a) Millbrook Central School District (school or district name), (hereinafter "School" or "District" as appropriate) and Diffit, Inc. (hereinafter "Diffit") are parties to a contract or other written agreement, or are utilizing the services pursuant to the Privacy Policy and Terms and Conditions, pursuant to which Diffit will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the School or District for purposes of providing certain products or services to the School or District (the "Master Services Agreement" or "MSA").

(b) This Exhibit supplements the MSA to which it is attached, to ensure that the MSA conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement and a copy of the School or District's Bill of Rights for Data Security and Privacy signed by Diffit that the School or District is required by Section 2-d to post on its website.

(c) In consideration of the mutual promises set forth in the MSA, Diffit agrees that it will comply with all terms set forth in the MSA and this Exhibit. To the extent that any terms contained in the MSA, or any terms contained in another Exhibit(s) attached to and made a part of the MSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Diffit has an online or written Privacy Policy or Terms of Service (collectively, "Policies") that would otherwise be applicable to its customers or users of the products or services that are the subject of the MSA between the School or District and Diffit, to the extent that any terms of the Policies, that are or may be in effect at any time during the term of the MSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

As used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in

Section 2-d, from student records that Diffit may receive from the District pursuant to the MSA.

(b) “Teacher or Principal Data” means personally identifiable information, as defined in Section2-d, relating to the annual professional performance reviews of classroom teachers or principals that Diffit may receive from the District pursuant to the MSA.

(c) “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Diffit pursuant to the MSA.

(d) “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3. Confidentiality of Protected Data

(a) Diffit acknowledges that the Protected Data it receives pursuant to the MSA originates from the School or District and that this Protected Data belongs to and is owned by the School or District.

(b) Diffit will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the School or District’s policy on data security and privacy. The School or District will provide Diffit with a copy of its policy on data security and privacy upon request.

4. Data Security and Privacy Plan

As more fully described herein, throughout the term of the MSA, Diffit will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the School or District. Diffit’s Plan for protecting the School or District’s Protected Data includes, but is not limited to, its agreement to comply with the terms of the School or District’s Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by Diffit. Additional components of Diffit’s Data Security and Privacy Plan for protection of the School or District’s Protected Data throughout the term of the MSA are as follows:

(a) Diffit will implement all state, federal, and local data security and privacy requirements including those contained within the MSA and this Data Sharing and Confidentiality Agreement, consistent with the School or District’s data

security and privacy policy.

(b) Diffit will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the School or District under the MSA.

(c) Diffit will comply with all obligations contained within the section set forth in this Exhibit below entitled “Supplemental Information about a Master Services Agreement between School or District and Diffit”. Diffit’s obligations described within this section include, but are not limited to: (i) its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Diffit by state and federal law and the MSA shall apply to the subcontractor, and (ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the MSA.

(d) Diffit has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e) Diffit will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Diffit will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

(f) Diffit will also have the following reasonable, administrative, technical, operational, and physical safeguards in place throughout the term of the MSA, which are described at https://web.diffit.me/privacy-policy.

5. Notification of Breach and Unauthorized Release

(a) Diffit will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Diffit has discovered or been informed of the breach or unauthorized release.

(b) Diffit will provide such notification to the District by contacting

Elliot Garcia, Assistant Superindendent for Business and Personnel (name and title) by email at elliot.garcia@millbrookcsd.org (email address) or by calling 845-677-4200 Ext 1102 (phone number).

(c) Diffit will cooperate with the District and provide as much information as possible directly to the School or District about the incident, including but not limited to: a description of the incident, the date of the incident, the date Diffit discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, if a District, instead of one school, the schools within the District affected, what Diffit has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Diffit representatives who can assist affected individuals that may have additional questions.

(d) Diffit acknowledges that upon initial notification from Diffit, the School or District, as the educational agency with which Diffit contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Diffit agrees not to provide this notification to the CPO directly unless requested by the School or District or otherwise required by law. In the event the CPO contacts Diffit directly or requests more information from Diffit regarding the incident after having been initially informed of the incident by the School or District, Diffit will promptly inform the School or District.

6. Additional Statutory and Regulatory Obligations

Diffit acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the School or District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the MSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); i.e. they need access in order to assist Diffit in fulfilling one or more of its obligations to the School or District under the MSA.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the MSA to which this Exhibit is attached.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Diffit using the information to carry out Diffit's obligations to the School or District and in compliance with state and federal law, regulations and the terms of the MSA, unless: (i) the parent or eligible student has provided prior written consent; or (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to the School or District no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e) Use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g) To comply with the School or District's policy on data security and privacy, Section 2-d and Part 121.

(h) To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i) To notify the School or District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Diffit or its assignees or subcontractors in violation of applicable state or federal law, the School or District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the MSA and this Exhibit.

(j) To cooperate with the School or District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k) To pay for or promptly reimburse the School or District for the full cost of

notification, in the event the School or District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Diffit or its subcontractors or assignees.

Diffit and this New York School or District are committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the School or District informs the school community of the following:

Parents and eligible students can expect the following:

1. A student's personally identifiable (PII) information cannot be sold or released for any commercial purposes.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws, such as NYS Education Law § 2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of personally identifiable information PII, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Contact at School or District: Elliot Garcia, Assistant Superindendent (name and title) by email: elliot.garcia@millbrookcsd.org(email address), or by phone: 845-677-4200 Ext 1102(phone number). Complaints should be submitted in writing via email. Complaints may also be submitted to NYSED online atwww.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, by email toprivacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or

unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with Diffit that receive PII will address statutory and regulatory data privacy and security requirements.

BY Diffit, Inc.

Name: Adam Black

Title: Co-Founder

Signature: Adam Black

Date: 2025-04-17

Supplemental Information about this Master Services Agreement between School or District and Diffit

School or District has entered into a MSA with Diffit, which governs the availability to the School or District of the following products or services: Diffit software, and/or apps, and/or technology tools, and/or web-services.

Pursuant to the MSA (which includes a Data Sharing and Confidentiality Agreement), the School or District may provide to Diffit, and Diffit will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used:
The exclusive purpose for which Diffit is receiving Protected Data from the School or District is to provide the School or District with the functionality of the products or services listed above. Diffit will not use the Protected Data for any other purposes not explicitly authorized above or within the MSA.

Oversight of Subcontractors:
In the event that Diffit engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the MSA (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Diffit under the MSA and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The MSA commences on 4/14/2025 and expires on 8/1/2030.
- Upon expiration of the MSA without renewal, or upon termination of the MSA prior to its expiration, Diffit will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Diffit or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the School or District, Diffit will assist the School or District in exporting all Protected Data previously received back to the School or District for its own use, prior to deletion, in such formats as may be requested by the School or District.

- In the event the MSA is assigned to a successor Diffit (to the extent authorized by the MSA), the Diffit will cooperate with the School or District as necessary to transition Protected Data to the successor to Diffit prior to deletion.

- Neither Diffit 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, Diffit and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the School or District 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 the School or District to Diffit, by contacting the School or District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of data provided to Diffit by following the appeal process in the District's applicable Plan.

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

Encryption of Protected Data:
Diffit (and, 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 that complies with Section 2-d of the New York Education Law.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
HMGGS-YMUQP-MD2J3-W8S7D

DOCUMENT COMPLETED BY ALL PARTIES ON
17 APR 2025 20:20:27 UTC

SIGNER	TIMESTAMP	SIGNATURE
ADAM BLACK EMAIL ADAM@DIFFIT.ME	SENT 17 APR 2025 04:47:58 UTC VIEWED 17 APR 2025 20:20:16 UTC SIGNED 17 APR 2025 20:20:27 UTC	 IP ADDRESS 135.180.249.231 LOCATION OAKLAND, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
17 APR 2025 20:20:16 UTC