EXHIBIT A: New York Ed Law 2-d

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Copiague Public Schools

Including Parental Bill of Rights for Data Security and Privacy

And Supplemental Information about a Master between Copiague School District and Achieve3000, Inc.

1. Purpose

(a) Copiague Public Schools and Achieve3000, Inc. are parties to a contract or other written agreement, or are utilizing the services pursuant to the Privacy Policy and Terms of Service, pursuant to which Achieve3000, Inc. 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 Copiague School District for purposes of providing certain products or services to the District (the "Master Agreement").

(b) This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement and a copy of the Copiague School District's Parental Bill of Rights for Data Security and Privacy signed by Achieve3000, Inc. that the District is required by Section 2-d and other New York law to post on its website

(c) In consideration of the mutual promises set forth in the Master Agreement, Achieve3000, Inc. agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in another Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of the Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that Achieve3000, Inc. has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the Copiague School District and Achieve3000, Inc., to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, 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 Achieve3000, Inc. may receive from the Copiague School District pursuant to the Master Agreement.

(b) "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Achieve3000, Inc. may receive from the Copiague School District pursuant to the Master Agreement.

(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 Copiague School District by Achieve3000, Inc. pursuant to the Master Agreement.

(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) Achieve3000, Inc. acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the Copiague School District and That this Protected Data belongs to and is owned by the School or District.

(b) Achieve3000, Inc. 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 Copiague School District's policy on data security and privacy. The Copiague School District will provide Achieve3000, Inc. 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 Master Agreement, Achieve3000, Inc. will have a Data Security and Privacy Plan in place to protect the Confidentiality, privacy and security of the Protected Data it receives from Copiague School District. Achieve3000, Inc.'s Plan for protecting the Copiague School District 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 Achieve3000, Inc.. Additional components of Achieve3000, Inc.'s Data Security and Privacy Plan for protection of the School or District's Protected Data throughout the term of the Master Agreement are as follows:

(a) Achieve3000, Inc. will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the Copiague School District data security and privacy policy.

(b) Achieve3000, Inc. will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the Copiague School District under the Master Agreement.

(c) Achieve3000, Inc. will comply with all obligations contained with the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between Copiague School district and Achieve3000, Inc. ". Achieve3000, Inc. 's obligations described within this section include, but are not limited to: (i) it's obligation to require subcontractor or other authorized person or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Achieve3000, Inc. by state and federal law and the Master Agreement shall apply to the subcontractor, and (ii) it's 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 Master Agreement.

(d) Achieve3000, Inc. has provided or will provide training on the requirements of 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) Achieve3000, Inc. will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Achieve3000, Inc. will provide prompt notification to the Copiague School 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.

5. Notification of Breach and Unauthorized Release

(a) Achieve3000, Inc. will promptly notify the School or District of any breach or unauthorized release of Protected Data it has received from the Copiague School District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Achieve3000, Inc. has discovered or been informed of the breach or unauthorized release.

(b) Achieve3000, Inc. will provide such notification to the School or District by Contacting ~~Jason Strumwasser, Director of Technology by email at jstrumwasser@copiague.net or by calling 631-842-4015 x 513.~~the current District contact on file with Achieve3000, Inc.

(c) Achieve3000, Inc. will cooperate with the Copiague School District and provide as much information as possible directly to the Copiague School District

about the incident, including but not limited to: a description of the incident, the date of the incident, the date Achieve3000, Inc. 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 the Achieve3000, Inc. 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 Achieve3000, Inc. representatives who can assist affected individuals that my have additional questions.

(d) Achieve3000, Inc. acknowledges that upon initial notification from Achieve3000, Inc., the Copiague School District, as the educational agency with which Achieve3000, Inc. contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Achieve3000, Inc. agrees not to provide this notification the CPO directly unless requested by the School or District or otherwise required by law. In the event the CPO contact Achieve3000, Inc. directly or requests more information from Achieve3000, Inc. regarding the incident after having been initially informed of the incident by the District, Achieve3000, Inc. will promptly inform the Copiague School District.

6. Additional Statutory and Regulatory Obligations

Achieve3000, Inc. 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 Master Agreement and 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 interest 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 Achieve3000, Inc. in fulfilling one or more of its obligations to the Copiague School District under the Master Agreement.

(b) To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.with the understanding Vendor retains aggregate, deidentified, anonymized information for improvement, research and development purposes.

(c) To not disclose any Protected Data to any other party, except for authorized representatives of Achieve3000, Inc. using the information to carry out Achieve3000, Inc.'s obligations to the Copiague School District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless: (k) the parent or eligible student has provided prior written consent as provided by the District: or (ii) the disclosure is required by statue or court order and notice of the disclosure is provided to the 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 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 Copiague School 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 of facilitate its use or disclosure by any other party for any marketing or commercial purpose of permit another party to do so.

(i) To notify the Copiague School 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 Achieve3000, Inc. or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the School or District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit.

(j) To cooperate with the Copiague School 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 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 or a breach or unauthorized release of Protected Data attributed to Achieve3000, Inc. or its subcontractors or assignees.

Achieve3000, Inc. and the Copiague School 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 I 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 Copiague School District: District by contacting Jay Strumwasser, Director of Technology by email at jstrumwasser@copiague.net or by calling 631-842-4015 x 513.

6. 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 to privacy@nysed.gov, or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

8. 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.

9. Educational agency contract with Achieve3000, Inc. that receive PII will address statutory and regulatory data privacy and security requirements.

3rd Party Representative: Kimberly Harvey

Signature: Kimberly A. Harvey

Title: VP Strategic Services

Date: 11/28/2022

Supplemental Information about this Master Agreement between School or District and Achieve3000, Inc.

School or District has entered into a Master Agreement with Achieve3000, Inc., which governs the availability to the School or District of the following products or services: Actively Learn software, and/or apps, and/or technology tools, and/or web-services.

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the School or District may provide to Achieve3000, Inc., and Achieve3000, Inc. 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 Used:
The exclusive purpose for which Achieve3000, Inc. 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. Achieve3000, Inc. will not use the Protected Data for any other purposes not explicitly authorized above or within the Master Agreement.

Oversight of Subcontract:
In the event that Achieve3000, Inc. engages subcontractors or other authorized person or entities to perform one or more of it's obligations under the Master Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized person 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 Achieve3000, Inc. under the Master Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination of Expiration:

- The Master Agreement commences on _____ and may be terminated by either party upon request to the other party.

- Upon expiration of the Master Agreement without renewal, or upon termination of the Master Agreement prior to its expiration, upon written request Achieve3000, Inc. will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Achieve3000, Inc. or any of its subcontractors or other authorized person or entities to whom it has disclosed Protected Data. If requested in writing by the School or District, Achieve3000, Inc. will assist the School or District in exporting all Protected Data previously received back to the School or District for it's own use, prior to deletion, in such formats as may be requested by the School or District.

- In the event the Master Agreement is assigned to a successor (to the extent authorized by the Master Agreement), the Achieve3000, Inc. will cooperate with the School or District as necessary to Transition Protected Data to the successor to Achieve3000, Inc. prior deletion.

- Neither Achieve3000, Inc. 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 deidentified Protected Data, on any storage medium whatsoever.~~ Upon written request, Achieve3000, Inc. and/or its subcontractors or other authorized person or entities to whom it has disclosed Protected Data, as applicable, will provide the School or District with a certification form an appropriate officer that these requirements have been satisfied in full.

McGraw Hill LLC Data Privacy and Security Guidelines

This Data Privacy and Security Guidelines (**"DPSG"** or **"Security Guidelines"**) document sets forth the duties and obligations of McGraw Hill (defined below) with respect to Personal Information (defined below). In the event of any inconsistencies between the DPSG and the Agreement (defined below), the parties agree that the DPSG will supersede and prevail. Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions.

    a. **"Agreement"** means the Agreement for the Services between the McGraw Hill LLC entity (**"McGraw Hill"**) and Subscriber incorporating the Privacy Notice to which these Security Guidelines are referenced and made a part thereof.

    b. **"Applicable Laws"** means federal, state and international privacy, data protection and information security-related laws, rules and regulations applicable to the Services and to Personal Information.

    c. **"End User Data"** means the data provided to or collected by McGraw Hill in connection with McGraw Hill's obligations to provide the Services under the Agreement.

    d. **"Personal Information"** means information provided to McGraw Hill in connection with McGraw Hill's obligations to provide the Services under the Agreement that (i) could reasonably identify the individual to whom such information pertains, such as name, address and/or telephone number or (ii) can be used to authenticate that individual, such as passwords, unique identification numbers or answers to security questions or (iii) is protected under Applicable Laws. For the avoidance of doubt, Personal Information does not include aggregate, anonymized data derived from an identified or identifiable individual.

    e. **"Processing of Personal Information"** means any operation or set of operations which is performed upon Personal Information, such as collection, recording, organization, storage, use, retrieval, transmission, erasure or destruction.

    f. **"Third Party"** means any entity (including, without limitation, any affiliate, subsidiary and parent of McGraw Hill) that is acting on behalf of, and is authorized by, McGraw Hill to receive and use Personal Information in connection with McGraw Hill's obligations to provide the Services.

    g. **"Security Incident"** means the unlawful access to, acquisition of, disclosure of, loss, or use of Personal Information.

    h. **"Services"** means any services and/or products provided by McGraw Hill in accordance with the Agreement.

2. Confidentiality and Non-Use; Consents.

    a. McGraw Hill agrees that the Personal Information is the Confidential Information of Subscriber and, unless authorized in writing by Subscriber or as otherwise specified in the Agreement or this DPSG, McGraw Hill shall not Process Personal Information for any purpose other than as reasonably necessary to provide the Services, to exercise any rights granted to it under the Agreement, or as required by Applicable Laws.

    b. McGraw Hill shall maintain Personal Information confidential, in accordance with the terms set forth in this Security Guidelines and Applicable Laws. McGraw Hill shall require all of its employees authorized by McGraw Hill to access Personal Information and all Third Parties to comply with (i) limitations consistent with the foregoing, and (ii) all Applicable Laws.

    c. Subscriber represents and warrants that in connection with any Personal Information provided directly by Subscriber to McGraw Hill, Subscriber shall be solely responsible for (i) notifying End

Users that McGraw Hill will Process their Personal Information in order to provide the Services and (ii) obtaining all consents and/or approvals required by Applicable Laws.

3. Data Security.

   McGraw Hill shall use commercially reasonable administrative, technical and physical safeguards designed to protect the security, integrity, and confidentiality of Personal Information. McGraw Hill's security measures include the following:

   a. Access to Personal Information is restricted solely to McGraw Hill's staff who need such access to carry out the responsibilities of McGraw Hill under the Agreement.

   b. Access to computer applications and Personal Information are managed through appropriate user ID/password procedures.

   c. Access to Personal Information is restricted solely to Subscriber personnel based on the user role they are assigned in the system (provided, however, that it is the Subscriber's responsibility to ensure that user roles match the level of access allowed for personnel and that their personnel comply with Applicable Law in connection with use of such Personal Information).

   d. Data is encrypted in transmission (including via web interface) and at rest at no less than 256-bit level encryption.

   e. McGraw Hill or a McGraw Hill authorized party performs a security scan of the application, computer systems and network housing Personal Information using a commercially available security scanning system on a periodic basis.

4. Data Security Breach.

   a. In the event of a confirmed Security Incident, McGraw Hill shall (i) investigate the Security Incident, identify the impact of the Security Incident and take commercially reasonable actions to mitigate the effects of any such Security Incident, (ii) timely provide any notifications to Subscriber or individuals affected by the Security Incident that McGraw Hill is required by law, subject to applicable confidentiality obligations and to the extent allowed and/or required by and not prohibited by Applicable Laws or law enforcement.

   b. Except to the extent prohibited by Applicable Laws or law enforcement, McGraw Hill shall, upon Subscriber's written request and to the extent available, provide Subscriber with a description of the Security Incident and the type of data that was the subject of the Security Incident.

5. Security Questionnaire.

   Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill shall respond to security questionnaires provided by Subscriber, with regard to McGraw Hill's information security program applicable to the Services, provided that such information is available in the ordinary course of business for McGraw Hill and it is not subject to any restrictions pursuant to McGraw Hill's privacy or data protection or information security-related policies or standards. Disclosure of any such information shall not compromise McGraw Hill's confidentiality obligations and/or legal obligations or privileges. Additionally, in no event shall McGraw Hill be required to make any disclosures prohibited by Applicable Laws. All the information provided to Subscriber under this section shall be Confidential Information of McGraw Hill and shall be treated as such by the Subscriber.

6. Security Audit.

   Upon written request by Subscriber, which request shall be no more frequently than once per twelve (12) month period, McGraw Hill's data security measures may be reviewed by Subscriber through an informal audit of policies and procedures or through an independent auditor's inspection of security methods used within McGraw Hill's infrastructure, storage, and other physical security, any such audit to be at Subscriber's sole expense and subject to a mutually agreeable confidentiality agreement and at mutually agreeable

timing, or, alternatively, McGraw Hill may provide Subscriber with a copy of any third party audit that McGraw Hill may have commissioned.

7. Records Retention and Disposal.

    a. Subscriber may access, correct, and delete any Personal Information in McGraw Hill's possession by submitting McGraw Hill's Personal Information Request Form: https://www.mheducation.com/privacy/privacy-request-form.

    b. McGraw Hill will use commercially reasonable efforts to retain End User Data in accordance with McGraw Hill's End User Data retention policies.

    c. McGraw Hill will use commercially reasonable efforts to regularly back up the Subscriber and End User Data and retain any such backup copies for a minimum of 12 months.