

**DATA PRIVACY AGREEMENT
BRIGHTON CENTRAL SCHOOL DISTRICT**

and

Bedford, Freeman & Worth Publishing Group, LLC

This Data Privacy Agreement ("DPA") is by and between the Brighton Central School District ("EA"), an Educational Agency, and Bedford, Freeman & Worth Publishing Group, ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means, in connection with the Services used hereunder, personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services identified in Schedule 1 attached hereto and made a part of hereof ("Services") to the EA pursuant to a contract dated July 22, 2024 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8

NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services and as set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

The EA understands and agrees that the Contractor will process PII in connection with the use of the Services by EA and its authorized users. Accordingly, the EA hereby grants to Contractor a license to: (i) to use all such PII as reasonably required to provide the Services; and (ii) de-identify (as defined in FERPA) the data obtained hereunder and analyze it to improve Contractor's educational products and services, including to create aggregated or statistical insights and baseline reports that are not identifiable to individuals or institutions for use in Contractor's other educational products and services. The rights granted in (ii) shall survive the expiration or termination of this DPA and override any deletion/destruction/return obligations herein

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor agrees to maintain an Enterprise Information Security & Privacy program based on industry best practice (ISO 27001/27002 and NIST).

5. Right of Review and Audit.

During the term of this Agreement, without undue delay following Contractor's receipt of a written request from the EA, no more than once in any twelve-month period, and subject to the execution of a mutually agreed upon non-disclosure agreement, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, during the term of this DPA, but no more than once in any twelve month period, without undue delay following Contractor's receipt of a written request from the EA, Contractor shall permit the EA to perform a remote audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. To verify Contractor's compliance with its security obligations hereunder. The scope of such remote audit shall be mutually agreed upon by Contractor and the EA and shall be conditioned upon Contractor and the EA executing a mutually agreed upon non-disclosure agreement. Such remote audit will occur during normal business hours. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing such remote audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond a reasonable period following Contractor's receipt of a written request from the EA after the expiration or termination of the Service Agreement to destroy such PII, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly required by law. As applicable, without undue delay following Contractor's receipt of a written request from the EA after the expiration or termination of the Service Agreement, Contractor shall destroy all PII. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII

cannot be read, or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

- (b) Without undue delay following Contractor's receipt of a written request from the EA after the Contractor's destruction of data, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (c) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent legally permissible and available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: Eric Jordan

Title: Director of Technology Services

Address: 2035 Monroe Ave.

City, State, Zip: Rochester, NY 14618

Email: Eric_Jordan@bcasd.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is caused by the failure of the Contractor or its Subcontractors to materially perform its obligations under this DPA.

14. Notification to Individuals.

Where a Breach of PII occurs and such Breach is caused by the failure of the Contractor to materially perform its obligations under this DPA, Contractor shall pay for or promptly reimburse the EA for the full cost incurred by the EA (which the EA is legally required or incur) in connection with the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement,

Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail with respect to such conflict, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.


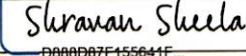
EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY:  <small>Signed by:</small>
Eric Jordan	Shravan Sheela <small>D000D07F155041F</small>
Director of Technology Services	VP Finance
Date: 8/27/24	Date: 8/26/2024 1:29 PM EDT

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: Eric Jordan, 2035 Monroe Avenue, Rochester, NY 14618, Eric_Jordan@bcasd.org (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 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 PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

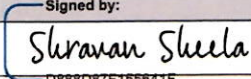
CONTRACTOR	
[Signature]	Signed by: 
[Printed Name]	D888D87F155641F... Shравan Sheela
[Title]	VP. Finance
Date:	8/26/2024 1:29 PM EDT

EXHIBIT B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE
INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Bedford, Freeman & Worth Publishing Group, LLC
Description of the purpose(s) for which Contractor will receive/access PII	Contractor will receive / access PII for the purpose of providing the Services and as set forth in the Agreement
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date: July 1, 2024 Contract End Date: June 30, 2025 This DPA shall apply to the contract term stated therein and any future service agreements between the parties.
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Without undue delay following Contractor’s receipt of a written request from the EA after the expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • • Securely delete and destroy PII.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: The data will be stored in the Contractor's servers in Amazon Web Services, and Contractor will use reasonable administrative, technical, and physical security measures designed to protect the data against unauthorized access or loss. The security measures shall include data encryption with no less than data being encrypted both at rest and while in transit. Furthermore, Contractor agrees to maintain an Enterprise Information Security & Privacy program based on industry best practice (ISO 27001/27002 and NIST).</p>
Encryption	Data will be encrypted while in motion and at rest.

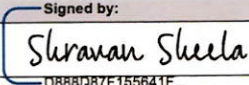
CONTRACTOR	
[Signature]	<p>Signed by:</p> 
[Printed Name]	Shravan Sheela
[Title]	VP. Finance
Date:	8/26/2024 1:29 PM EDT

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<p>We at Macmillan recognize that U.S. educational institutions are subject to the requirements of the Family Educational Rights and Privacy Act ("FERPA"). Accordingly, we understand the importance of maintaining the security of any "personally identifiable information" from "education records" covered by FERPA and provided to us by the institution ("FERPA information"). All data transmitted to us by students and/or instructors, such as registration information, polling responses, quiz results, grades, and assessments, is transmitted utilizing TLS encryption. Such data is held by Amazon Web Service's (AWS) cloud computing infrastructure utilizing state-of-the-art security systems (as more fully described at http://aws.amazon.com/security/). We have implemented the appropriate administrative, technical and physical safeguards necessary to protect against unauthorized access, destruction, use, modification or disclosure of FERPA Information.</p>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>While we do not yet certify with any individual enterprise standard (e.g. SSAE 16), we maintain strong administrative, technical, and physical safeguards aligned with information security and privacy controls designed to protect systems and data,</p>

		<p>including personally identifiable information, against unlawful or unauthorized destruction, loss alteration, access, disclosure, or use. Our environment is cloud-based and thus we ascribe to security best practices for designing cloud-based environments, including establishing a DMZ. We utilize Web Application Firewalls for enhanced protection. In addition, our Information Security program is based on the ISO/IEC 27001/02, ISO 27017 and NIST 800-37. We routinely run scans that cover OWASP Top 10/ SANS Top 25 and are integrating that into our development process.</p>
<p>3</p>	<p>Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.</p>	<p>Our Head of Security is responsible for the development and delivery of a comprehensive information security and privacy program for the organization. Information Security and Privacy training must be completed by all new hires within the first 30 days of employment. Annual Information Security and Privacy training is mandatory for all employees and contractors. Additional Information Security and Privacy training (e.g. online training courses via our internal training portal) and awareness campaigns are provided to users throughout the year. Vendors/subcontractors are under substantially similar security restrictions as Macmillan employees with respect to the Achieve system or data to which they are granted access. These are called out and agreed contractually. All subcontractors are required to follow all of Macmillan Learning's data policies as well as all federal and state laws governing confidentiality of student data.</p>

4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All employees and subcontractors are required and contractually obligated to follow all of Macmillan Learning's data policies as well as all federal and state laws governing confidentiality of student data.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	We have formal escalation and incident response processes that are followed. In the event that we experience a confirmed data breach, in addition to abiding by all applicable laws and using reasonable business efforts, we will also work to minimize the effect of the breach as well as work with potentially impacted institutions to the extent reasonably possible.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	With the exception of de-identified and/or anonymized data and after receipt of written request from the Institution, we shall ensure that all PII in Protected Data stored on Macmillan Learning systems is securely destroyed pursuant to the National Institute of Standards and technology (NIST) SP 800-88 Guidelines for Media Sanitization.
7	Describe your secure destruction practices and how certification will be provided to the EA.	With the exception of de-identified and/or anonymized data and after receipt of written request from the Institution, we shall ensure that all PII in Protected Data stored on Macmillan Learning systems is securely destroyed pursuant to the National Institute of Standards and technology (NIST) SP 800-88 Guidelines for Media Sanitization
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We agree materially but would have to review.