

DATA PRIVACY AGREEMENT

Medina Center School District

and

Jostens, Inc.

This Data Privacy Agreement ("DPA") is by and between the Median Central School District ("EA"), an Educational Agency, and Jostens, Inc. ("Contractor"), collectively, the "Parties".

RECITALS

WHEREAS, the Contractor has agreed to provide the EA with certain services ("Services") pursuant to a contract dated 8/1/2021 and expires on 7/31/2022 ("Service Agreement"); and

WHEREAS, in order to provide the Services, the Contractor may receive from the EA and the EA may provide the Contractor student data, teacher and/or principal data (collectively, "Protected Data"), protected by several New York and federal laws and regulations, among them, the Federal Educational and Privacy rights 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); Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the laws referred to above.

NOW THEREFORE, the Parties agree as follows:

ARTICLE I: DEFINITIONS

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

1. **Authorized Users:** Contractor's employees and non-employee recipients.

2. **Breach:** The unauthorized acquisition, access, use, or disclosure of Protected Data by or to a person not authorized to acquire, access, use, or receive it.
3. **Commercial or Marketing Purpose:** The sale of student data, teacher or principal data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve or market products or services to students.
4. **Contract, agreement or written agreement:** A binding agreement between an EA and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
5. **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.
6. **Education Record:** An education record as defined in FERPA and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
7. **Educational Agency:** A school district, board of cooperative educational services, school, charter school or the New York State Education Department.
8. **Eligible Student:** A student eighteen years or older.
9. **Encrypt or Encryption:** Methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached, as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304.
10. **Non-Employee Recipients:** Contractor's nonemployee agents, consultants and/or subcontractors engaged in the provision of Services pursuant to the Service Agreement.
11. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
12. **Parent:** A parent, legal guardian or person in parental relation to the student.
13. **Release:** Shall have the same meaning as Disclose.
14. **Student:** Any person attending or seeking to enroll in an educational agency.
15. **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, regarding students from the student records of an educational agency.
16. **Subscribing EA:** An Educational Agency that was not party to the original Services Agreement and who accepts the General Offer of Privacy Terms.

- 17. Teacher or Principal 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 § 2012(c).

ARTICLE II: DATA PROTECTION

- 1. Purpose.** Contractor is permitted to have access to Protected Data solely and exclusively for the purpose set forth in the Service Agreement as outlined in Exhibit B, the parents bill of rights for data privacy and security supplemental information. Contractor agrees to hold the Protected Data in strict confidence, and not to disclose it for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this Agreement.
- 2. Ownership of Protected Data.** Contractor has no property or licensing rights or claims of ownership to any Protected Data.
- 3. Right to Review.** The EA has the right to review Contractor's procedures, practices and controls related to the protection of Protected Data. To that end, upon request, Contractor will make available for review policies, procedures, practices and documentation related to the protection of Protected Data. In addition, Contractor may be required to undergo an audit of its privacy and security controls performed by an independent third party at Contractor's expense, and provide the audit report to an EA, or in the alternative, provide EA with a recent independent audit report on privacy and security controls.
- 4. Parent and Eligible Student Access.** Education Law §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 twenty-five (25) calendar days to the EA's requests for the Contractor to facilitate such review by a Parent or Eligible Student, and as applicable, 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 immediately notify the EA and refer the Parent or Eligible Student to the EA.
- 5. Compliance with Law.** Contractor agrees to maintain the confidentiality of Protected Data in accordance with applicable New York and federal laws, rules, and regulations including, but not limited to, FERPA; COPPA; PPRa; IDEA; Education Law § 2-d; 8 NYCRR Part 121; and EA policies relating to data privacy and security as amended, including, without limitation, those

data privacy and security policies that are implemented subsequent to the execution of this DPA and which are provided to Contractor.

6. **Bill of Rights for Data Privacy and Security.** As required by §2-d of the Education Law, 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 for the Service Agreement and append it to this DPA. Pursuant to Education Law §2-d, the EA is required to post the completed Exhibit B on its website.
7. **Contractor's Authorized Users.** Contractor shall only disclose Protected Data to Authorized Users who need to know the Protected Data in order to carry out the Services, provided that such disclosure shall be made only to the extent justifiable by such need, and shall adopt and maintain administrative, physical and technical security and privacy controls and protocols that ensure access only to Authorized Users. Contractor shall ensure that all such Authorized Users comply with the terms of this DPA. Contractor agrees that upon request by the EA, it will provide the EA with the names and affiliations of the Non-Employee Recipients to whom it proposes to disclose, or has disclosed, Protected Data. Contractor shall ensure that each Non-Employee Recipient is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this DPA.
8. **Subcontractor.** Where use of a subcontractor is authorized, Contractor shall, by written agreement, ensure that all requirements set forth herein apply to all subcontractors performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to Protected Data. Such written agreements shall include provisions that (a) state that work performed by the subcontractor must be in accordance with the terms and conditions of this DPA, and (b) ensure that the subcontractors will abide by all applicable data protection and security requirements, including but not limited to those requirements included in the Service Agreement, this DPA, and applicable New York and federal laws and regulations. Contractor shall take full responsibility for the acts and omissions of its subcontractors. Contractor shall examine the data security and privacy measures of its subcontractors before it agrees to utilize the subcontractor and shall periodically do so for as long as the subcontractor is being utilized to fulfill the Contractor's responsibilities under the Service Agreement. If at any point a subcontractor fails to comply with the requirements of this DPA, Contractor shall: so notify the EA; take all necessary steps to retrieve all Protected Data received or stored by such subcontractor and ensure that such data has been securely deleted and destroyed in accordance with this DPA; and remove such subcontractor's access to Protected Data. In the event there is an incident in which the subcontractor compromises Protected Data, Contractor shall follow the Data Breach reporting requirements set forth herein.

- 9. Destruction of Data.** Nothing in the Service Agreement shall authorize Contractor to maintain Protected Data after termination of the Service Agreement. Upon written request, Contractor shall provide the EA a written certification of the secure deletion and/or destruction of Protected Data held by the Contractor and its Non-Employee Recipients no later than ten (10) business days after the Service Agreement terminates. If applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer, in a format agreed to by the parties, Protected Data to the EA or the EA's successor contractor, at the EA's option and written direction provided to the Contractor prior to or immediately upon the expiration or termination of the Service Agreement. Contractor shall thereafter, with regard to all Protected Data (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all Protected Data maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Non-Employee Recipients, securely delete and/or destroy such Protected Data in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, and direct its Non-Employee Recipients to do the same.. Hard copy media must be shredded or destroyed such that Protected Data cannot be read or otherwise cannot be reconstructed, and electronic media must be cleared, purged, or destroyed such that the Protected Data cannot be retrieved. Redaction is specifically excluded as a means of data destruction.
- 10. No Sale or Commercial Use.** Contractor agrees that it will not sell Protected Information; use or disclose Protected Information for purposes of receiving remuneration, whether directly or indirectly; use or disclose Protected Information for marketing, commercial or advertising purposes or facilitate its use or disclosure by any other party for such purposes; or use or disclose Protected Information to develop, improve or market products or services to students, or permit another party to do so.
- 11. Disclosure Limitations.** Unless as permitted by this DPA, Contractor shall not disclose any Protected Data to any party who is not an Authorized User. Notwithstanding the foregoing, Contractor may disclose Protected Data if such disclosure is required by statute or court order and the Contractor makes a reasonable effort to notify the EA of the order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the Protected Data is disclosed, unless such disclosure to the EA is expressly prohibited by statute or court order.
- 12. Encryption.** Contractor shall use industry best practices to preserve and protect Protected Data from unauthorized disclosure. Contractor shall use Encryption technologies to protect Protected Data at rest, on file storage, database storage, or on back-up media, and in transit/motion.
- 13. Data Security and Privacy Plan.** Contractor shall maintain reasonable administrative, technical and physical safeguards that conform to federal, State and EA mandates, the NIST

Cybersecurity Framework or an equivalent standard that meets and or exceeds its requirements, and generally recognized industry standards and practices to protect the security, confidentiality and integrity of Protected Data in its custody. Contractor is required to have a Data Security and Privacy Plan that, at a minimum, complies with 8 NYCRR Part 121, and is acceptable to the EA. Contractor's data privacy and security safeguards are described in greater detail in its' Data Privacy and Security Plan attached hereto as Exhibit C.

- 14. Training.** Contactor shall ensure that all Authorized Users who have access to Protected Data have received or will receive training on the federal and state laws governing confidentiality of such data and understand the privacy and data security obligations of this DPA prior to receiving access.
- 15. Data Breach Reporting.** Contractor shall notify the EA of any breach of security resulting in an unauthorized release or disclosure of Protected Data by Contractor or its Authorized Users in violation of applicable state or federal law and/or this DPA without unreasonable delay, but no later than ten (10) business days after discovery of the breach or unauthorized release. 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 first class mail, postage prepaid, at the address set forth on Exhibit B. Such notification shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery, if known; a description of the types of Personally Identifiable Information affected, an estimate of the number of records affected, a brief description of the Contractor's investigation or plan to investigate, and contact information for representatives who can assist the EA. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The breach and unauthorized release of certain Personally Identifiable Information protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- 16. Cooperation with Investigations.** Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, to protect the integrity of any investigations into a breach or unauthorized release of Protected Data. 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.
- 17. Notification Costs.** Where a breach or unauthorized release of Protected Data occurs that is attributable to Contractor or any of its Authorized Users, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to parents, students, teachers, and/or principals, in accordance Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: 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, the Service Agreement, and any of Contractor's terms of service or privacy notices that apply to the Services, the terms and conditions of this DPA shall prevail. In addition, this DPA and all its Exhibits shall be deemed a part of and incorporated into the Service Agreement but shall survive the termination of the Service Agreement in the manner set forth herein.
2. **Entire Agreement.** This DPA constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.
3. **Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of New York, without regard to conflicts of law principles. The state and federal courts located in New York will have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this DPA, the Service Agreement referenced in this DPA, or the transactions contemplated hereby.
4. **Execution.** This DPA as well as attached exhibits A, B and C 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. This DPA as well as the attached exhibits A, B and C may be executed by signatures to facsimile copy or electronic transmittal documents in lieu of an original or machine generated or copied document, and each signature thereto shall be and constitute an original signature, as if all Parties had executed a single original document.

JOSTENS, INC.Signature: Tammy WhitakerPrinted Name: Tammy WhitakerTitle/Position: VP and GM YearbookDate: 4/13/2021**MEDINA CENTRAL SCHOOL DISTRICT**Signature: Anthony MorenoPrinted Name: Anthony MorenoTitle/Position: Data Protection OfficerDate: 4/13/21

EXHIBIT A - EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Medina Central School District is 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 District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, 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 New York State is available for public review at the following website <http://www.nysed.gov/student-dataprivacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Medina Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract; Page 2 of 2
- 2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- 3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and 6) Address how the data will be protected using encryption while in motion and at rest.

JOSTENS, INC.

Signature: Tammy Whitaker

Printed Name: Tammy Whitaker

Title/Position: VP and GM Yearbook

Date: 4/13/2021

MEDINA CENTRAL SCHOOL DISTRICT

Signature: Anthony Moreno

Printed Name: Anthony Moreno

Title/Position: Data Protection officer

Date: 4/13/21



**EXHIBIT B - BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PROTECTED DATA**

The Educational Agency is required to post information to its website about its agreements with third-party contractors that will receive Protected Data pursuant to Education Law §2-d and Part 121.3 of the Commissioner's Regulations.

Contact information for notifications of any breach of security resulting in an unauthorized release or disclosure of Protected Data by Contractor or its Authorized Users is as follows:

Medina CSD Data Protection Officer (DPO):

- Name: Anthony Moreno
- Email: amoreno@medinacsd.org
- Phone: 585-798-1534
- Address: 1 Mustang Drive, Medina NY 14103

Name of Vendor	Jostens, Inc.
Products	yearbooks
Description of Services	Printing and publication of yearbooks; assist with marketing as authorized to do so by the school
List of Protected Data elements	Personal Identification Information such as name, address, school year, etc.
Service Agreement Term (Start and End Dates)	
Subcontractors	_____ Contractor will utilize subcontractors in accordance with the terms of the DPA and shall require, pursuant to written agreement, that its subcontractors adhere to the same or greater data protection obligations imposed on the contractor by state and federal laws and regulations, and this DPA. <u> X </u> Contractor will not utilize subcontractors.



Data Transition and Secure Destruction	Upon expiration or termination of the contract, Contractor shall: ✓ Securely transfer data to EA, or a successor Contractor at the EA's option and written discretion, in a format agreed to by the parties, ✓ Securely delete and destroy data, and ✓ Certify to EA that secure deletion is complete.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of Protected Data may do so by contacting the EA's Data Protection Officer, who will review all such requests. If a correction to data is deemed necessary, Contractor will work with the EA to make such corrections, as applicable.
Secure Storage	Contractor will securely store Protected Data in a manner briefly described below (state storage location and the protections taken to ensure the data will be protected, and data and security privacy risks mitigated, in a manner that does not compromise the security of the data): Data is stored at Jostens controlled facilities and follows NIST guidelines
Encryption and Data Security	<u> X </u> Data will be encrypted while in motion and at rest. <u> </u> Data will be protected with the additional data security and privacy practices outlined in greater detail in Contractor's Data Privacy and Security Plan.

JOSTENS, INC.

Signature: Tammy Whitaker
Printed Name: Tammy Whitaker
Title/Position: VP and GM Yearbook
Date: 4/13/2021

MEDINA CENTRAL SCHOOL DISTRICT

Signature: Anthony Moreno
Printed Name: Anthony Moreno
Title/Position: Data Protection officer
Date: 4/13/21



EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency is required to ensure that all contracts with a third-party contractor include an acceptable Data Security and Privacy Plan, pursuant to Education Law § 2-d and Part 121.6 of the Commissioner's Regulations. Contractor must complete the following or provide a plan that at a minimum, addresses the following.

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the contract, as consistent with the educational agency's data security and privacy policy.	See Jostens Cybersecurity Compliance Program
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect personally identifiable information that you will receive under this contract.	See Jostens Cybersecurity Compliance Program
3	Certify compliance with the requirements set forth in the Supplemental Information to the Parents Bill of Rights.	See Jostens Cybersecurity Compliance Program
4	Specify how Authorized Users have been trained or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.	Upon hiring and annually
5	Outline contracting process that ensures that Authorized users are bound by written agreement to the requirements of this DPA, at a minimum.	See Jostens Cybersecurity Compliance Program



6	Specify how you will manage any data security and privacy incidents that implicate Protected Data and describe any specific plans you have in place to identify breaches and unauthorized disclosures, and to meet your obligations to report incidents to the educational agency.	See Jostens Cybersecurity Compliance Program
7	Describe how will data be transitioned to the educational agency when no longer needed by Contractor to provide Services, if applicable.	See Jostens Cybersecurity Compliance Program
8	Describe secure destruction practices and how certification will be provided to the educational agency.	See Jostens Cybersecurity Compliance Program

JOSTENS, INC.

Signature: Tammy Whitaker
Printed Name: Tammy Whitaker
Title/Position: VP and GM Yearbook
Date: 4/13/2021

MEDINA CENTRAL SCHOOL DISTRICT

Signature: Anthony Moreno
Printed Name: Anthony Moreno
Title/Position: Data Protection Officer
Date: 4/13/21