

DATA PRIVACY AGREEMENT

Shenendehowa Central School District

and

New York State School Music Association (NYSSMA)

This Data Privacy Agreement ("DPA") is by and between the Shenendehowa Central School District ("EA"), an Educational Agency, and NYSSMA ("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 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 ("Services") to the EA pursuant to a contract dated November 1, 2021 ("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 set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

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 and the EA's policies. 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 CyberSecurity Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, 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, Contractor may be required to undergo an 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. 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 an 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 subcontractors retain PII or retain access to PII.

9. Data Return and 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 the period of providing Services to the EA, unless such

retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. 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.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) 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 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:

Rebecca Carman
Shenendehowa District Privacy Officer
5 Chelsea Place
Clifton Park, NY 12065
carmrebe@shenschools.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 attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of 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, 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: <i>[Signature]</i> Rebecca Carman	BY: <i>[Signature]</i> David Gaines <small>AC56A8A1938ED649DA1A7BF6C3D5998D contractworks</small>
<i>[Printed Name]</i> Rebecca Carman	<i>[Printed Name]</i> David Gaines
<i>[Title]</i> DPO	<i>[Title]</i> Executive Director
Date: 11/3/21	Date: 11/03/2021

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, place of birth, social security number, biometric record & mother's maiden name, which when linked to or combined with other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or any information requested by a person if the educational agency or institution reasonably believes that person knows the identity of the student to whom the education record relate
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 Shenendehowa Central School District, Director of Policy & Community Development/Data Protection Officer, 5 Chelsea Place, Clifton Park, NY 12065. (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]	<i>David Gaines</i> AC56A8A1938ED649DA1A7BF6C3D5998D contractworks
[Printed Name]	David Gaines
[Title]	Executive Director
Date:	11/03/2021

EXHIBIT B

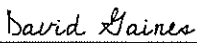
BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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	The New York State School Music Association (NYSSMA)
Description of the purpose(s) for which Contractor will receive/access PII	NYSSMA uses student data for selection of students in honor ensembles and student evaluations.
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 _11/1/21_____ Contract End Date 6/30/22_____
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	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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.
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	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input checked="" type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other: 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 is stored locally on servers and on two offsite data centers, one in Pennsylvania and the other in Utah. The data is encrypted at rest and in-transit, remote access to the data is secured by multifactor identification, the least privileged access policy is in place. There is a secure password policy and password rotation policy in place.

Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	 AC56A8A1938ED649DA1A7BF6C3D5998D contractworks
[Printed Name]	David Gaines
[Title]	Executive Director
Date:	11/03/2021



NYSSMA®

A State Unit of NAFME, National Association for Music Education

DATA PRIVACY AND CYBERSECURITY FRAMEWORK POLICY

April, 2021

New York State School Music Association (NYSSMA) has chosen to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This risk-based approach allows NYSSMA to proactively address and better manage cybersecurity risks to its business while the organization continuously evaluates the constantly changing landscape of cyber threats.

The NIST Cybersecurity Framework uses five core functions as the tenants of its framework – Identify, Protect, Detect, Respond and Recover - and NYSSMA has included some of its internal processes in this summary, listed below.

Identify: NYSSMA seeks to continuously evaluate which systems, assets, data and capabilities need to be protected. This evaluation process is owned by the Executive Director.

Protect: NYSSMA takes a layered approach to security and does not believe that any single service, device or software is capable of complete protection. Individual protections include, but are not limited to:

- NYSSMA employees are trained in basic security principles and to recognize social engineering techniques
- All NYSSMA servers, computers and laptops have antivirus software and managed detection and response software installed to continuously monitor for malicious behavior and activity
- All NYSSMA servers, computers and laptops are kept up to date with the latest security and critical patches, applied on a rolling basis
- NYSSMA uses hardware firewall appliances at its network gateway as well as a dedicated VPN appliance to provide secure remote access that is encrypted
- All NYSSMA servers and critical business data are backed up on a rolling basis throughout each day with encrypted copies stored offsite in redundant data centers
- NYSSMA has a secure password and authentication policy in place, including for its wireless networks
- NYSSMA employs the use of multifactor authentication in front of all sources of data, including email access and its internal network resources
- NYSSMA limits employee access to specific data required for specific functions
- NYSSMA controls physical access to its computers and network infrastructure

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org

Detect: NYSSMA continuously monitors its security services and physical network, looking for anomalies and other events that may present potential security issues. Any detected events are analyzed and processes are continually improved based on new information gathered.

Respond: It is the policy of NYSSMA to respond to each cybersecurity event on a case-by-case basis, taking into consideration the specific circumstances and extent to which the event occurred. In order to best protect NYSSMA and its clients, all qualifying events are to be reported to the Executive Director to ensure that a response plan is initiated, should it be deemed necessary. A response plan includes, but is not limited to:

- Communication with relevant stakeholders or other key personnel, including status updates as needed
- Taking steps to immediately quarantine any breach or incident to mitigate impact
- Studying each incident to incorporate lessons learned, updating strategies accordingly

Recover: NYSSMA plans to recover from a cybersecurity event either during or after an incident. Aside from addressing and mitigating the specific circumstances of each incident, NYSSMA maintains a Business Continuity and Disaster Recovery plan to address any significant business disruptions that may occur.



NYSSMA[®]

A State Unit of NAFME, National Association for Music Education

8 NYCRR Part 121	
121.2 Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with Federal and State law and the educational agency's data security and privacy policy.	
121.3(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information. The supplemental information must be developed by the educational agency and include the following Information:	
121.3(b)(1) What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	NYSSMA uses student data for selection of students in honor ensembles and student evaluations.
121.3(b)(2) Will the organization use subcontractors? If so, how will the organization 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 State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d)?	Yes – NYSSMA will use subcontractors. NYSSMA will obtain contracts with it's subcontractors including data confidentiality requirements as well as compliance with Ed Law 2-d, 8 NYCRR Part 121 and the NIST CSF.
121.3(b)(3) What is the duration of the contract including the contract's expected commencement and expiration date? Describe 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 educational agency, and/or whether, when and how the data will be destroyed).	NYSSMA does contract directly with school districts through it's student registration process. The duration of the contract is year to year and commences as districts participate and terminate when the event is over. The duration of the contract is determined on an event by event basis. The contract commences on July 1, and terminates on June 30 th of each year. When the engagement with the district terminates, NYSSMA will return or destroy the data at the direction of the school district.

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org



NYSSMA®

A State Unit of NAFME, National Association for Music Education

<p>121.3(b)(4)</p> <p>how can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected;?</p>	<p>Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to NYSSMA, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA).</p>
<p>121.3(b)(5)</p> <p>Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.</p>	<p>The data is stored locally on servers and on two offsite data centers, one in Pennsylvania and the other in Utah.</p> <p>The data is encrypted at rest and in-transit, remote access to the data is secured by multi-factor identification, the least privileged access policy is in place. There is a secure password policy and password rotation policy in place.</p>
<p>(6)address how the data will be protected using encryption while in motion and at rest.</p>	<p>The server itself the data volume is encrypted on the physical server and the back up technology is also encrypted. It is encrypted in transit back to those data centers. Staff laptops are encrypted.</p>
<p>121.6(a)Please submit the organization's data security and privacy plan that is accepted by the educational agency.</p>	<p>See attached.</p>
<p>121.6(a)(1)</p> <p>Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;</p>	<p>NYSSMA affirmatively states that it will maintain compliance with all State and Federal and local data security and privacy contract requirements consistent with the educational agency's data security and privacy policy.</p>
<p>121.6(a)(2)specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;</p>	<p>The data is encrypted at rest and in-transit, remote access to the data is secured by multi-factor identification, the least privileged access policy is in place. There is a secure password policy and password rotation policy in place. Please refer to the "Protect" section of the NYSSMA data privacy policy.</p>
<p>121.6(a)(3)demonstrate that the organization complies with the requirements of section 121.3(c) of this Part</p>	<p>NYSSMA will sign the education agency's Parent Bill of Rights.</p>
<p>121.6(a)(4)specify how officers or employees of the organization and its assignees who have</p>	<p>Refer to privacy policy. NYSSMA uses the "KnowBe4" training platform.</p>

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org



NYSSMA®

A State Unit of NAFME, National Association for Music Education

access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access;	
121.6(a)(5) specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;	Sub-contractors are used to process student data for the purposes of evaluation and honors ensemble participation. Sub-contractor management is defined in the privacy policy.
121.6(a)(6) specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;	The educational agency will be promptly notified of a breaches and unauthorized disclosure by the NYSSMA Executive Director. Breach management is defined in the privacy policy.
121.6(a)(7) describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	The school district will be notified of any transition to a successor contractor and data will be deleted or returned to the educational agency at the request of the school district.
121.9(a) In addition to all other requirements for third-party contractors set forth in this Part, each third-party contractor that will receive student data or teacher or principal data shall:	
121.9(a)(1) describe the organization's adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework;	NYSSMA aligns with the NIST CSF. Refer to the privacy policy.
121.9(a)(2) Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d ; and this Part;	Refer to the privacy policy.
121.9(a)(3) Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;	Refer to privacy policy.
121.9(a)(4) Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract;	Refer to the privacy policy. NYSSMA will only use student data for evaluations and honors ensembles.
121.9(a)(5) Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student;	NYSSMA will not disclose any personally identifiable information to any other party with out prior written consent, except to the extent

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org



NYSSMA®

A State Unit of NAFME, National Association for Music Education

<p>(i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or</p> <p>(ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.</p>	<p>that it is complying with State or Federal law, or regulation, unless required to do so by statute or court order.</p>
<p>121.9(a)(6)Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;</p>	<p>Refer to privacy policy.</p>
<p>121.9(a)(7) Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest; and</p>	<p>The server itself the data volume is encrypted on the physical server and the back up technology is also encrypted. It is encrypted in transit back to those data centers. Staff laptops are encrypted.</p>
<p>121.9(a)(8)Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.</p>	<p>NYSSMA will not sell personally identifiable information and will not use or disclose the information for any marketing or commercial purpose or permit another party to do so.</p>
<p>121.9(a)(b) Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.</p>	<p>Refer to privacy policy.</p>
<p>121.10(a) Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.</p>	<p>NYSSMA will promptly notify the school district, without unreasonable delay and within seven calendar days after the discovery of the breach in the most expedient manner possible.</p>
<p>121.10(c) Affirmatively state that the organization will cooperate with educational</p>	<p>NYSSMA will cooperate with educational agencies and law enforcement to protect the</p>

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org



NYSSMA[®]

A State Unit of NAFME, National Association for Music Education

agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	integrity of investigations into the breach or unauthorized release of personally identifiable information.
121.10(f) Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	NYSSMA will pay for or promptly reimburse the educational agency for the full cost of such notification.

Dr. David A. Gaines, Executive Director, 718 The Plain Road, Westbury, NY 11590-5956

Phone: 516-997-7200 ext. 10 • Fax: 516-997-1700 • Email: executive@nyssma.org • Website: www.nyssma.org