

## DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING  
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY  
AND  
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

### 1. Purpose

- (a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

### 2. Definitions

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

- (d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

### 3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

### 4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: [

## PRIVACY POLICY

Music Sales Digital Services, LLC (hereinafter "MusicFirst") is committed to safeguarding your privacy online. For the purpose of this

policy, MusicFirst defines the term “User” as an individual or entity with which MusicFirst has an established relationship, and the term “Visitor” as an individual that visits its front-end website. Any information stored on MusicFirst’s platform is treated as confidential. All information is stored securely and is accessed by authorized personnel only. MusicFirst implements and maintains appropriate technical, security, and organizational measures to protect personal data against unauthorized or unlawful processing and use, and against accidental loss, destruction, damage, theft, or disclosure.

Please read the following policy (“Privacy Policy”) to understand how your personal information will be treated as you make full use of our website and services.

#### NOTICE CONCERNING MINORS

Minors (as defined under the laws of THEIR jurisdiction or residence) are not eligible to use these services without the express permission and/or supervision of their parent or guardian. MusicFirst does not knowingly collect personal information from any minor without parental consent, and we will not use this information if we discover that it has been provided without such consent. This site and service has been designed so that student users are not required to disclose their contact information. Parents and teachers are encouraged to discuss these policies and online safety practices with their children and students.

#### FERPA

MusicFirst 180 Madison Avenue, 24th Floor New York, NY 10016 United

The Family Educational Rights and Privacy Act of 1974 (“FERPA”) is a federal law that states that an educational institution must establish a written institutional policy concerning the confidentiality of student

education records and the fact that students must be notified of this statement of policy and their rights under the legislation. Your student



records are protected by FERPA policy and the MusicFirst staff has been trained to follow and enforce this policy.

**FERPA Block** – A FERPA Block allows you to protect the privacy of your information. It prevents the release of all your private information, including the ability of MusicFirst to communicate with you by phone should you need to discuss information in your record. If you have a FERPA Block in place, you can communicate with us by email.

In accordance with FERPA, MusicFirst Users have the following rights:

1. The right to inspect and review education records covered by FERPA.
2. The right to challenge (seek correction of) the contents of these records.
3. The right to a formal hearing, if necessary, for a fair consideration of such a challenge.
4. The right to place an explanatory note in the record in the event that a

challenge of contents is unsuccessful.

5. The right to control, with certain exceptions, the disclosure of the contents

of the records.

6. The right to be informed of the existence and availability of the institutional policy covering FERPA rights.
7. The right to report violations of FERPA legislation to MusicFirst and any

applicable administrative body. The name and address of the Office that administers FERPA is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC, 20202-4605.

Users who wish to inspect and review their education records may do so by submitting a written request to MusicFirst at 180 Madison Avenue, 24th floor, New York NY 10016. MusicFirst must respond with 45 days of the request by arranging an appointment for the User to review the requested data.

A User may challenge the contents of an education record which they consider to be inaccurate, misleading, or otherwise in violation of their privacy rights. Users may initiate a challenge by submitting a written

request to MusicFirst at 180 Madison Avenue, 24th floor, New York NY 10016 which shall attempt to resolve the problem through informal discussions. If a challenge to a record is not satisfactorily resolved by this procedure, the User will be informed of their right to a formal hearing, the procedures to be followed concerning such a hearing, and its composition. A User requesting a hearing will be notified in writing of the date, place, and time of their hearing.

The hearing board will consist of individuals who are disinterested parties but who may be MusicFirst employees. The decisions of the hearing board will be communicated to the User. Decisions of the hearing panel are final. If decisions of the hearing board are unsatisfactory to the User, the User may place in the education record a

statement commenting on the information contained in the record and setting forth any reason for disagreeing with the decision of the hearing panel. If MusicFirst discloses the contested portion of the record, it must also disclose the User's statement.

Users will be notified of their FERPA rights annually by e-mail and this policy will be reviewed by MusicFirst every two years.

### **New York Education Law §2-d**

MusicFirst is committed to protecting the confidentiality, integrity and security of student, teacher and staff data, consistent with the provisions of New York Education Law §2-d. MusicFirst is committed to working diligently to ensure our practices are in alignment with the finalized provisions of New York Education Law §2-d. Upon request, MusicFirst will append a Parents' Bill of Rights to our agreement with any New York State school district. New York State district administrators should reach out to their MusicFirst account manager to add a Parents' Bill of Rights to their MusicFirst agreement.

## **How and when do you consent to this Privacy Policy?**

By submitting personal information to us (through the use of this website and/or registering an account) you agree that MusicFirst may collect, use and disclose such personal information in accordance with this Privacy Policy and as permitted or required by law. If you do not agree with these terms, do not provide any personal information to us. If you refuse or withdraw your consent, or if you choose not to provide us with any required personal information, we may not be able to provide you with the services of this website and services that can be offered on our site only if we have access to that certain personal information.

Page 2 of 3

## **What personally identifiable information does MusicFirst collect from you?**

MusicFirst collects information in several ways. By visiting this website, Visitors consent to the collection and use of their personal data. If you don't agree with the terms set out herein, please do not visit this website. If required by applicable law, we will seek your explicit consent to process personal data collected on this website or volunteered by you.

Some personal information is gathered when you register for an account. When submitting a request for an account, MusicFirst asks for your first and last name and asks that you create a unique user name and password. For teacher, administrator, and teacher accounts MusicFirst will also request your email address and/or other contact information. When using the service Whether you are a Visitor or User, MusicFirst may passively collect your GPS location through your device, record your IP address, or use cookies. When passively collecting data in this manner, MusicFirst does not draw any conclusions about the data subject. Some of this information is necessary to take advantage of our

services; some of the information that is collected is used to improve our services and offer targeted services announcements.

If you contact MusicFirst we may keep a record of that correspondence. Whenever MusicFirst collects personal information we make an effort to include a link to this Privacy Policy on that page.

### Data Processing in the European Economic Area (EEA)

A MusicFirst “Data Region” is a set of data centers located within a defined geographical area where User data is stored. Personal data is not transmitted between Data Regions. For Users with accounts located in MusicFirst’s European Data Region, all processing of personal data is performed in accordance with privacy rights and regulations following the EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the “Directive”), and the implementation

Page 21 of 37

of the Directive in local legislation. From May 25, 2018, the Directive and local legislation based on the Directive will be replaced by the Regulations (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, known as the General Data Protection Regulation (“GDPR”), and MusicFirst’s processing will take place in accordance with GDPR.

MusicFirst processes personal data as both a Processor and Controller, as defined in the Directive and the GDPR. Consequently, MusicFirst processes all data provided by its Users with accounts in its European Data Region, in the European Economic Area (“EEA”) only.

### **What are some things we do NOT do?**



We do not and will not, at any time, request your credit card information, login name, or password, in an unsecure or unsolicited e-mail or telephone communication and we will not request the contact information, including email, of a minor. Additionally we will not request any confidential or personal information through social networking sites, including, but not limited to, Twitter, LinkedIn, Pinterest, FourSquare, and Facebook.

MusicFirst does not use automatic decision-making or profiling.

### **What happens when you call or write to our Customer Service?**

When you call or write to our Customer Service, we may collect contact information, such as name, phone number, mailing address and/or e-mail address to process a service request. No such information will be collected directly from a minor.

### **What are cookies and how does MusicFirst use them?**

Page 2 of 7

MusicFirst may use cookies to store and sometimes track information about you. A “cookie” is a small amount of data that is sent to your browser from a web server and stored on your computer’s hard drive. Generally, we use cookies to:

*Monitor our services* – It may be necessary from time to time for MusicFirst to monitor and/or track site usage as part of an internal audit of our services.

Portions of this audit may be performed through the use of temporary cookies placed on your computer by the MusicFirst site.

*Facilitate login* – Cookies may be used to collect and store login information to facilitate future logins.

Some cookies used by MusicFirst are strictly necessary and essential in order to enable you to move around the site and service and use its features. Without these cookies, services you have asked for cannot be provided; they are deleted when you close your browser. Performance cookies are used to collect information in an anonymous form about how visitors use the service. MusicFirst may also use your IP address to help diagnose problems with its server and to improve its service and may perform IP lookups to determine which domain you are coming from to more accurately gauge user demographics. Information received in these forms is not combined with other information about you from any other source.

**DO NOT TRACK.** MusicFirst does not respond to Do Not Track Requests.

### **How does MusicFirst use your information and with whom is your information shared?**

MusicFirst's primary goal in collecting personal information is in providing you the best service possible through its site. The majority of

Page 2 of 3

information that is collected about you is for the purpose of verifying account registration and delivering relevant services and announcements.

MusicFirst may retain your account information for as long as permitted by law and as long as is necessary to permit you to use our services without the requirement of resubmitting the same information.

Except as provided herein, MusicFirst shall not sell, rent, trade or otherwise transfer any personal and/or traffic data or communications content to any third party without your explicit permission, unless it is

obliged to do so under applicable laws or by order of the competent authorities

Your information may be used to effect a corporate transaction, in connection with the sale, merger, spin-off or other corporate reorganization of our corporation, where the information is provided to the new controlling entity in regular course of business. In the event of such an occurrence, every effort will be made by MusicFirst to inform you of the transfer of your personal information.

Your information may be disclosed as is required by our insurers and by regulatory agencies or to employees, contractors, consultants, and agents of MusicFirst to perform necessary actions in the normal course of business. No more information than is required in these circumstances will be provided.

### **What about linked websites?**

MusicFirst's web pages and applications may contain links that will let you leave the MusicFirst service and access another website. These "linked websites" are not under the control of MusicFirst and it is possible that these websites have different privacy policies. This policy applies solely to personal information that is acquired on this website (MusicFirst.com) and through the MusicFirst application and service. MusicFirst accepts no responsibility or liability for your use or disclosure of personal information to linked websites.

Page 2 of 3

### **What are your choices regarding collection, use, and distribution of your information?**

The disclosure of very limited personal information is required to create an account on our site, which is required to access certain services. If you

do not wish to disclose the requisite information you are free to discontinue use of the MusicFirst website and service.

You also have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies MusicFirst may not be displayed or function in the way intended by MusicFirst.

Right of confirmation – Users and Visitors will have the right granted by the European legislator to obtain from MusicFirst the confirmation as to whether or

not personal data concerning him or her his being processed. If a data subject wishes to avail him or herself of this right of confirmation, he or she may, at any time, contact our Data Protection Officer.

Right of access – Users and Visitors will have the right granted by the European legislator to obtain from MusicFirst free information about his or her personal data stored at any time and a copy of this information. Furthermore, the European directives and regulations grant the data subject access to the following information: (1) the purpose of the processing; (2) the categories of personal data concerned; (3) the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations; (4) where possible, the anticipated period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (5) the existence of the right to request from MusicFirst rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object

Page 2 of 3

to such processing; (6) the existence of the right to lodge a complaint with a supervisory authority; (7) where the personal data is not collected from the data subject, any available information as to its source; (8) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and anticipated consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data is transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

**If a data subject wishes to avail him or herself of this right of access, he or she may at any time contact our Data Protection Officer.**

Right of rectification – Each User or Visitor shall have the right to obtain from MusicFirst without undue delay, the rectification of inaccurate personal data concerning him or her; and to complete incomplete data.

Right of restriction of processing – Each User or Visitor shall have the right to obtain from MusicFirst restriction of processing where: (1) the accuracy of the personal data is contested; (2) processing is unlawful and the data subject requests restriction rather than erasure; (3) MusicFirst no longer needs the personal data for the purpose of the processing; or (4) the data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of MusicFirst override those of the data subject.

Page 2 of 3

Right to withdraw consent – Each Visitor and User shall have the right to withdraw his or her consent to processing of his or her personal data at any time by contacting our Data Protection Officer.

### **How long is your personal information stored?**

MusicFirst will retain your personal information and IP information as long as is permitted by applicable laws and regulations or as long as necessary to achieve the purpose of storage of such information, whichever is shorter. If a storage purpose is not applicable, or if a storage period prescribed by the European legislator or other competent legislator expires, the personal data will be routinely blocked or erased in accordance with legal requirements.

### **What is MusicFirst’s policy on allowing you to update, correct, or delete your personally identifiable information?**

If you wish to update, correct, or delete any of the information about you stored by MusicFirst you can do so by visiting the account settings on your account profile. For all other information changes or requests, please send an inquiry

to [support@musicfirst.com](mailto:support@musicfirst.com)

MusicFirst Users have control of the purpose for collecting data, and the duration for which the personal data may be kept. Users with an active account will therefore have the responsibility to delete data when required.

MusicFirst, as the Controller of personal data, shall, at any time, provide information upon request to each User or Visitor as to what personal data is stored about that data subject. In addition, MusicFirst shall correct or erase

personal data upon request. When a User's account is terminated or expired, all personal data collected through the MusicFirst platform will be deleted, as required by applicable law.

Page 2 of 3

### **What security precautions are in place to protect the loss, misuse, or alteration of your information?**

MusicFirst shall take the appropriate organizational and technical measures to protect the personal information and IP data provided to it or collected by it necessary to comply fully with any and all applicable laws, obligations, and regulations.

Unfortunately, no data transmission over the Internet can be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, MusicFirst cannot ensure or warrant the security of any information you transmit to us or from our online products or services, and you do so at your own risk. Once we receive your transmission, we make our best effort to ensure its security on our systems.

### **What else should you know about your privacy?**

If you choose to use the MusicFirst website and service you should be aware that any information transmitted electronically via the World Wide Web or wirelessly might not be secure. MusicFirst assumes no liability for the loss of any information that you transmit to us via the World Wide Web.

We may release personal information when we believe in good faith that release is necessary to comply with a law; to enforce or apply our Terms of Use and other policies; or to protect the rights, property, or safety of MusicFirst, our employees, our users, or others.

MusicFirst's Data Protection Officer



Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892

MusicFirst has a "Data Protection Officer" who is responsible for matters relating to privacy and data protection. This Data Protection Officer can be reached at the following address:

MusicFirst

Page 2 of 3



Attn: Dr Jim Frankel

180 Madison Avenue, 24th floor, New York NY 10016  
info@musicfirst.com

### Complaints

The Information Commissioner's Office (ICO) is an independent body responsible for making sure that organizations comply with the Data Protection Act. The ICO also deals with concerns raised by members of the public about the way in which organizations look after personal information and deal with subject access requests.

You can complain to the ICO if an organization:

- fails to respond to your request for disclosure
- refuses your request
- fails to send you all of the information you asked for



- fails to comply with the 40-day time limit for disclosure

The ICO will always expect you to have raised your concerns with the organization before submitting a complaint.

The ICO has a form on its website which you can use to make your complaint. When you send the form to the ICO, include all the communications you've had with the organization about your request for disclosure, including copies of the documents raising your concerns.

If you have this saved electronically, you can submit the form and

Page 219 of 317

the correspondence by email to [casework@ico.org.uk](mailto:casework@ico.org.uk).

If you only have paper copies of the correspondence, you will need to send it along with the form to Customer Contact, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

You can call the ICO helpline on 0303 123 1113 (local rate).

You should make a complaint to the ICO within three months of your last proper contact with the organization concerned.

When is the effective date of this policy, and what about future modifications?

This Privacy Policy is effective as of March 28th, 2018. MusicFirst reserves the right to make changes, deletions, modifications, or provide supplements to this policy from time to time. Changes will apply to the

information collected after the date of changes as well as to existing information held by us and will take effect immediately upon publication, unless otherwise stated in writing by MusicFirst. You agree that the express acceptance by you, or your continued use of the MusicFirst website after publication of changes, shall constitute your acceptance of the Privacy Policy.

If you have any further questions or concerns, please feel free to contact us by email at: [support@musicfirst.com](mailto:support@musicfirst.com), or in writing at:

MusicFirst

180 Madison Avenue, 24th floor, New York NY 10016

(b)

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] \_\_\_\_\_ will  will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
  - (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
  - (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
  - (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
    - (i) the parent or eligible student has provided prior written consent; or
    - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
  - (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
  - (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
  - (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
  - (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.
6. **Notification of Breach and Unauthorized Release**
- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.


**EXHIBIT D (CONTINUED)**

**PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the 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 the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 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 the 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/data-privacy-security/report-improper-disclosure>.

**BY THE VENDOR:**

  
 \_\_\_\_\_  
 Signature

\_\_\_\_\_  
**Jason Panucci**  
 Printed Name  
 Account Manager

\_\_\_\_\_  
 Title

**Date** 5/19/2023

## EXHIBIT D (CONTINUED)

### SUPPLEMENTAL INFORMATION

#### ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT BETWEEN ERIE 1 BOCES AND [MUSICFIRST]

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with [MusicFirst which governs the availability to Participating Educational Agencies of the following Product(s):

*MusicFirst Classroom and optional software components*

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

**Exclusive Purpose for which Protected Data will be Used:** The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: [

WISE MUSIC GROUP LTD dba MusicFirst agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with BOCES Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by WISE MUSIC GROUP LTD and is set forth below. Data is handled by M24/7/365 server monitoring. Dedicated IPs. SSL certificates. McAfee Quarterly PCI security scans.

#### **Duration of MLSA and Protected Data Upon Expiration:**

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other

authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, 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). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

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

**Encryption of Protected Data:** Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.



Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892