Sight Reading Factory

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and GraceNotes, LLC **("Vendor")** are parties to a contract dated 9/28/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, SightReadingFactory.com subscriptions ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means GraceNotes, LLC.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to thisAddendum.

5. Vendor EmployeeTraining

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)** GraceNotes, LLC.
Date 9/29/23	**Date** 9/28/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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 at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained 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, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)** GraceNotes, LLC.
Date	**Date**
9/29/23	9/28/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

Privacy Policy

Sight Reading Factory (the "Service," or "SRF") is a product of GraceNotes, LLC ("GraceNotes," "we," or "us"), a Virginia limited liability company. This Privacy Policy ("Policy") governs the use of all user accounts, as well as all activity on, in, or related to the Service, the SRF web site, and interactions with us.

GraceNotes considers its users' privacy a priority.

GraceNotes will not sell, trade, or assign any customer information to third parties. If GraceNotes shares any such information with a third party, it will be in accordance with the terms of this privacy policy and for the limited purposes that we discuss below. If you have any questions, concerns or comments regarding this privacy policy, you may contact us at the email and address posted at the end of this policy statement. We are committed to addressing your privacy or security questions or concerns.

For purposes of this Privacy Policy and GraceNotes' Terms of Service, the phrase "user account" refers to a Sight Reading Factory® account created by an individual or family for personal or family use. It can also refer to an account created at the prompting of an educational institution or district that has purchased Sight Reading Factory® accounts for its student users.

Information Collected by GraceNotes

You must create an account on our website in order to use Sight Reading Factory®'s online services. You may be part of a school system that is providing access to Sight Reading Factory® as a benefit to its students and has provided a registration code. Or you may wish to use Sight Reading Factory® independently as part of your private music practice. Both scenarios are described below.

If your school system has contracted with GraceNotes to use its services, a teacher or authorized school official must first register on the Sight Reading Factory®'s website so that student accounts can be linked to the school's account. The school official is asked to enter the following information during registration: first name, last name, and email. In order to process payment for the school system, either credit card or Paypal account information is collected. Payment information is not stored by GraceNotes. Students age 12 and under who are creating a school account are asked to enter the following information during registration: first name, last initial, and username. Users under 12 are prohibited from using an email address as their username (the "@" character is disallowed).

By default, students above the age of 12 must use an email as their username, and are allowed to provide a full last name. Sight Reading Factory allows administrators to opt-in to prohibiting use of email and last name for all students of any age. If the administrator chooses to prohibit this information, then students age 13 and older are asked to enter first name, last initial, and username. If the administrator chooses to allow this information, then students age 13 and older are asked to enter first name, last name, and email. Email address is used by us only for automating Forgot Password functionality, and is not shared with third parties.

Those signing up on behalf of Independent Sight Reading Factory® users age 12 and under are asked to enter the following information during registration: first name, last initial, and a parent's email address which will be the username. Students age 13 and older who are creating an individual account are asked to enter the following information during registration: first name, last name, and email. Payment information, via credit card or Paypal, is also requested from both groups. Payment information is not stored by GraceNotes.

As users participate in the Sight Reading Factory® online program, GraceNotes collects information about usage, history, session data, and preferences selected on the user's dashboard. Details associated with each practice composition, including the instrument selected and level of difficulty, are collected. Where user accounts are linked to a school system or private instructor, practice compositions assigned, including audio recordings, and teacher feedback are saved.

Exceptions From Information Collection

If students access Sight Reading Factory® through a learning management system ("LMS," for example Canvas or Blackboard), or a single sign-on ("SSO," for example Auth0 or OneLogin), GraceNotes will not collect any personally identifiable information about them.

Information collected directly from users

GraceNotes also collects information directly from users as they interact with the site. This student-generated data includes but is not limited to a user's choice of instrument, level and time signature, time spent playing a composition, selections made to customize a given assignment, and audio recordings of practice sessions. We may use student-generated and teacher-generated data to analyze student-generated data and provide the student and his or her teacher with periodic progress reports on performance, and to improve GraceNotes' offerings. If we ever need to collect information that is not generated from usage, GraceNotes will seek authorization of a parent, guardian, or school official prior to collecting such additional information from the user. In addition, we may aggregate your student's generated data with the generated data of other students for business related purposes. Aggregate information will be anonymous and will not allow individual users to be identified.

How GraceNotes will use the information collected from you

GraceNotes does not collect, maintain, use, or share student personal information beyond that needed for educational purposes, as authorized by parents and students. By 'educational purposes,' we mean services or functions that customarily take place at the direction of schools and teachers, that aid directly in instruction and practice of music education

Email Address: For some users over the age of 12 and school administration officials, email address will serve as login username. If email address is collected, it may be used to send a confirmation email upon registration and it may be used as an additional means of communicating about our services, including notifications of updates to the web site or its related policies. However, if a user signs up with a school system voucher, that user will not be added to the mailing list and email address provided will only be used for password reset. For users under the age of 12, an identifier set up at registration will serve as login username in lieu of email, and parental email provided for consent will only be used for password reset.

Student's Name: Student's name will be used to customize areas of the website, as well as to personalize the reports and updates to teachers or school administrators concerning student progress. Users 12 and under will only be asked for first name and last initial, whereas students 13 and older will be asked for first and last name.

Credit Card or PayPal Information: In order to collect payment for services provided, Stripe and PayPal services are offered. No payment data is stored in GraceNotes' database.

Participation Data: Participation history will be collected by GraceNotes for customer care, business development, and other operational purposes, including improvements to our services; however, such information will not be disclosed to third parties or used for advertising directly to student users.

Secondary Uses: Registration Information and other information may be used for ad-hoc data analysis and internal reporting on site usage. In all cases, the information will only be used to further our educational purposes, either internally by GraceNotes or shown to the user to whose account it pertains. Such information be aggregated as anonymous statistical information. GraceNotes will not sell, trade, or assign any personal information to third parties outside nor directly target any type of communication to a student.

Reviewing and changing your information

You may review and modify your account information at any time by using your password to access the site. An export of your account data can be provided upon request by writing to the address or email below. We provide this access to student personal information to parents and students for review and correction, either by direct request from student users, parents, or through a school or teacher. Please allow 5 business days for completion of your request.

Deleting your account, retention of data

A user who initially opens an account related to a school system can continue to maintain their user account after graduating from or leaving that school system. A user simply needs to pay the fee associated with maintaining the account when it is due in order to keep the account active. The account can persist in an inactive state if the user does not pay the maintenance fee. However, if at any time, a user decides they actively want to remove his or her account from GraceNote's user database, he or she can initiate a deletion request by writing to the address or email below. Please allow 5 business days for completion of your request. Where we do not receive a specific request for removal of account-related data from our database, GraceNotes' standard information retention practice and the limits of its obligation to retain data on inactive accounts is limited to two years.

Consent

For students who have received a school code from their school system in order to create an account, the school system has contracted with GraceNotes to collect the limited personal information described above from students for the use and benefit of the school and for no other commercial purpose. Based on this, GraceNotes provides the school system with full notice of its collection, use, and disclosure practices and presumes that the school's authorization for collection of students' personal information is based upon the school having obtained parental consent.

Users under the age 18 who are creating accounts independently outside of a school system must have parental consent. Parents are not contacted directly.

Password Protection

You will be asked to select a password to access GraceNotes services. Your password should be kept confidential. Your password will allow you to review and change the information we collect about you, or if you're a teacher or school administrator, it will allow you to review information about your students.

Protecting your information

No data transmissions over the internet can be guaranteed to be 100% secure, and, therefore, GraceNotes cannot completely ensure or warrant the security of any information you transmit to us.

As a third-party contractor to educational institutions, GraceNotes has adopted and will continue to align its practices with the National Institutes of Standards and Technology's Cybersecurity Framework ("NIST CSF"), as well as federal and state laws including laws referenced in this policy, and New York State Education Law § 2-d and its implementing regulations. Internal access to education records is limited to those GraceNotes employees or subcontractors who require it to provide the contracted services. We will:

maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII,
use encryption technology to protect data while in motion or in our custody from unauthorized disclosure, using controls as specified by the Secretary of HHS in guidance issued under Public Law 111-5, § 13402(h)(2).

More specifically, we have taken the following measures to protect the data from loss, misuse or alteration of information under our control.

Data in transit: All browser/server communications utilize HTTPS/TLS 1.1 protocol currently.
Browser/server communication protocols are reviewed and updated on a quarterly basis.
Data at rest: Passwords are stored using a hashing algorithm (bcrpyt) specifically designed for this purpose. Passwords are never stored or transmitted in an unencrypted format such that even Gracenotes does not have the ability to un-encrypt them.
Production environment access is limited to two site owners and is protected with two-factor authentication.
Automatic snapshot backups of the production database are retained for 7 days. Redundant full DDL backups are retained for 1 day.
Industry best practices are leveraged when coding the site and emphasis is placed on preventing attacks such as SQL injection.
If a data breach occurs that results in an unauthorized release of user data, Gracenotes is responsible for notifying the school district or, if not associated with a school district, the independent user within 72 hours from the time the data breach occurred. If the account is connected to a school district, the notification must be written and include what happened, when the breach occurred, when the breach was identified, a complete accounting of the data that was breached, the number of students or employees impacted, which students or employees were impacted, and steps taken to mitigate continued breach of data. If the account is not connected to a school district, Gracenotes will use the parent's email address of users under 12 and the student's email address for users over 12 to send notification of the data breach.

Please note that the Sight Reading Factory® website is hosted in the United States. If you are visiting from the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that you are transferring your personal data to the United States, which does not have the same data protection laws as the EU or other regions. By providing your personal data you consent to the use of your personal data for the uses identified above in accordance with this Privacy Policy and the transfer of your personal data to the United States as indicated above.

Your information and third parties

GraceNotes will not sell, trade, or assign any personal information that it collects to third parties. GraceNotes uses Google Analytics to track usage data. Geolocation is used at signup to estimate the user's timezone for end user reporting and formatting only. All data is aggregated and reported in the form of anonymous group statistics and in a manner that makes individual student users unidentifiable. GraceNotes' use of Google AdWords is completely separate from the website and no re-marketing to site visitors is done.

GraceNotes uses third party vendors and hosting partners to provide the necessary hardware and other technical contributions required to run SRF. Although we own the code, databases, and all rights to SRF and the Service, you retain all rights to your own data.

Except as provided in this Privacy Policy, GraceNotes will not disclose the information that it obtains from you to third parties without your express written permission, or where we believe, in good faith, that the law requires us to disclose the information. GraceNotes reserves the right to disclose personally identifiable information under certain circumstances, such as to comply with subpoenas, or when actions of any user are believed or alleged to violate the Terms of Service. As deemed necessary, in our judgment, we will share information in order to investigate illegal activities at any stage and in any capacity, such as suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service, or as otherwise dictated by law.

Notwithstanding anything to the contrary, as GraceNotes continues to develop its business, it might sell some or all of its assets. In such transactions, customer information is generally one of the transferred business assets. An acquiring company would be required to protect all information that GraceNotes collects from users in accordance with the terms of this Privacy Policy.

Unsolicited third-party promotional emails

GraceNotes will not send unsolicited third-party promotional emails.

Use of cookies

As a standard practice, GraceNotes uses “cookies”. A cookie is a small amount of data sent to your browser from our web server and stored on your computer, then sent back to the server by your browser each time you access our website. Cookies are used solely for the operations of our website and services, specifically to implement "remember me" functionality for login and to remember user settings on the "dashboard", i.e. preferences on sorting and displaying practice data. We do not use cookies to collect any personal information, nor do we use them for behavioral advertising, to build a student profile unrelated to the use of the Sight Reading Factory® website, or for any other reason. Cookies are required for the functioning of SRF. We use cookies to record session information as our users use the application, but we never use permanent cookies. Cookies cannot be used to gather personal information from your computer.

Sight Reading Factory® Mobile App

GraceNotes offers users the option of practicing via the mobile app in addition to the website. The mobile app is simply a front-end interface that connects to the same service behind the website and collects less user information than the website. All privacy policies explained here apply to the mobile app as well.

Children’s Online Privacy Protection Act

For our individual users or parents or legal guardians of a student, Congress has enacted a law called the Children’s Online Privacy Protection Act of 1998 (COPPA) that is designed to protect children’s privacy during use of the Internet. GraceNotes has implemented practices consistent with the guidelines provided by the Federal Trade Commission to date. GraceNotes will never knowingly request, obtain, use or disclose personally identifiable information or private content from anyone under the age of 13 without parental consent. Users who are seeking an account independently from a school system, will be asked to confirm that they have parental consent before starting registration.

If this question is answered affirmatively, we may receive personal information from children under the age of 13 in order to provide our services to them. GraceNotes does not share children's personally identifiable information with third parties. If you are a parent or legal guardian of a user under 13 you may, at any time, revoke your consent to allow your student to use GraceNotes' website, refuse to allow GraceNotes to further use or collect your student's personal information, or direct GraceNotes to delete all identifiable information regarding your student that you have provided. To do so, please contact our Privacy Officer at the contact information below. For administrative officials of our School Customers, to the extent that GraceNotes collects, uses, or discloses personal information from children under the age of 13, it is done in strict accordance with this Privacy Policy and for the sole purpose of providing services to the School Customer and student user. If you would like more information about COPPA, please go to https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

The Children's Internet Protection Act

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding support for Internet access or internal connections from the "E-rate" program — a program that makes certain technology more affordable for eligible schools and libraries. GraceNotes does not provide links to external resources or chat rooms and our site does not contain any offensive or inappropriate material. If you would like more information about CIPA, please go to http://www.fcc.gov/cgb/consumerfacts/cipa.html.

The Family Educational Rights and Privacy Act

Relevant for our users associated with a school system, the Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. GraceNotes helps our school district administrators be compliant with FERPA. Specifically:

Any sensitive online information is transmitted over secure channels
All student data is stored in ways such that it is not publicly accessible
Security audits are performed to ensure data integrity

GraceNotes does not share information with any third parties that could be used to personally identify students. If a school requests that student data be sent to a third party, with parental consent, GraceNotes will send the data to the school and never directly to the third party. If you would like more information about FERPA, please go to https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

The Student Online Personal Information Protection Act

The Student Online Personal Information Protection Act (SOPIPA) imposes rigorous rules on operators of websites or providers of internet services or mobile applications where the services are used primarily for "K-12 school purposes" and were designed and marketed for K–12 school purposes. Among other things, it prohibits the use of student data for targeted advertising on the website, service or app and the sale of student data. Operators of educational online services must also implement and maintain reasonable security procedures and practices, as well as protect that student data from unauthorized access, destruction, use, modification, or disclosure.

GraceNotes will not sell, trade, or assign any customer information to third parties. Targeted advertising is not done currently and is not planned for the future. GraceNotes has taken several precautions as described above in section 8 to protect user data from loss, misuse or alteration of information under our control.

If you would like more information about SOPIPA, please go to https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

A Word About the CCPA

We sometimes get questions about the California Consumer Privacy Act (effective starting in 2020). That law does not apply to SRF. We do not sell anyone's personal information. We do not therefore derive any revenue from selling consumers' personal information. We do not buy or sell personal information related to more than 50,000 consumers, households, or devices. We do not have gross annual revenues in excess of $25 million. As always, if you have any questions or concerns about how we collect and handle information, please contact us at support@sightreadingfactory.com"

Amendments

GraceNotes may amend this Privacy Policy from time to time. If updates are made, we will immediately advise users of this and obtain their consent. The application will redirect users to a page displaying the privacy policy, and not let them proceed without accepting the policy. Please review all revisions to the Privacy Policy. Your continued use of our website after the date that GraceNotes posts a notification of the update to our website will be deemed to be your agreement to the changed terms.

Contact Us

If you have any questions about your privacy or the security measures we have implemented, please contact our Privacy Officer at:

GraceNotes, LLC
1321 Upland Drive
Suite 12621
Houston, Texas 77043
Email: support@sightreadingfactory.com
Phone (U.S. and Canada): 888-433-7722

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by GraceNotes, LLC. (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated 9/28/2023 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to 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., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in _____ **(insert data format)** format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored Amazon S3, Reston, VA (**insert location**). The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: _____

Date: _9/28/2023_____