




Purchasing Department

209 Water Street  
Johnson City, TN 37601  
(423) 975-2716

## **ADDENDUM**

---

TO: All Prospective Vendors

FROM: Debbie Dillon,   
Director of Purchasing

SUBJECT: Addendum No. 2 RFP# 6629  
Electronic Health Records System Software

DATE: May 24, 2022

Consider this addendum an integral part of the above referenced solicitation:

See attached JCS Data Privacy Protection Agreement as referenced in the proposal documents.

All other specifications/requirements remain the same. **Vendor to acknowledge receipt of this addendum by initialing and returning the addendum notice with the return solicitation package or via e-mail if it has already been submitted.** Failure to acknowledge this addendum could be cause for rejection of your submittal. Any questions regarding addendum submittal please contact this office.

/dd



## Data Privacy/Protection Addendum

The Privacy Policy Addendum (hereinafter, the “Addendum”) is made and entered into on this \_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_, by and between \_\_\_\_\_, (“Company”), including any and all *Company* products utilized, and Johnson City Schools (“District”), a Tennessee public school district, and designed to supplement Company’s Terms of Service and Privacy Policy(s) otherwise applicable to the matters outlined herein. To the extent that any provision of the Terms and Service or Privacy Policy conflict with or contradict with this addendum, this Addendum shall govern, and the terms of the Agreement that conflict or are inconsistent with this Addendum shall be of no force or effect.

### 1. Definitions

- a. “District Data” includes all Personally Identifiable Information and other information that is not intentionally made generally available by the District on public websites or publications, including but not limited to business, administrative and financial data, intellectual property and student and personnel data and metadata.
- b. “End User” is defined as the individuals authorized by the District to access and use the Services provided by the Company under this Agreement.
- c. “Personally Identifiable Information” (or PII) includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; “personal information” as defined in the Tennessee Public Records Act, TCA § 10-7-503; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card

Industry Data Security Standards; other financial account numbers, access codes, and state- or federal- identification numbers such as driver's license, passport or visa numbers.

d. "Securely Destroy" is defined as taking actions that render data written on physical or electronic media unrecoverable by both ordinary and extraordinary means.

e. "Security Breach" is defined as an event in which District Data is exposed to unauthorized disclosure, access, alteration or use.

f. "Services" is defined as any good or services acquired by the District from the Company, including computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents via the Internet and used as part of a school activity.

g. "Mining District Data" is defined as to search through, access, or extract District Data, metadata, or information which is not necessary to accomplish the purpose(s) of this Agreement.

## **2. Rights and License in and to District Data**

The parties agree that as between them, all rights including all intellectual property rights in and to District Data shall remain the exclusive property of the District, and Company has a limited, nonexclusive license as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give Company any rights, implied or otherwise, to District Data, content, or intellectual property, except as expressly stated in the Agreement.

## **3. Data Privacy**

a. Company will use District Data only for the purpose of fulfilling its duties under this Agreement and will not share such data, including anonymized data, with or disclose it to any third party without the prior written consent of the District, except as required by law.

b. District Data will not be stored outside the continental United States without prior written consent from the District.

c. Company will provide access to District Data, including anonymized, only to its employees and subcontractors who need to access the data to fulfill Company obligations under this Agreement. Company will ensure that employees and subcontractors who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement. If Company will have access to “education records” for the District’s students as defined under the Family Educational Rights and Privacy Act (FERPA), Company acknowledges that for the purposes of this Agreement it will be designated as a “school official” with “legitimate educational interests” in the District education records, as those terms have been defined under FERPA and its implementing regulations, and Company agrees to abide by the FERPA limitations and requirements imposed on school officials. Company will use the education records only for the purpose of fulfilling its duties under this Agreement for District’s and its End Users’ benefit, and will not share such data with, or disclose it to, any third party except as provided for in this Agreement, required by law or authorized in writing by the District.

d. Company will not use District Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District.

e. Company agrees to assist District in maintaining the privacy of District’s data in Company’s possession as may be required by State and Federal law, including but not limited to the Protection of Pupil Rights Amendment (PPRA), the Children’s Online Privacy Protection Act (COPPA), and the Tennessee Public Records Act, TCA § 10-7-503.

f. Company is prohibited from building a personal profile of a student or employee, or mining District Data for any purposes other than those agreed to by the Parties; however, Company is not prohibited from using District Data for purposes of adaptive learning or customized education when used solely for the purpose of performing its obligations hereunder.

#### 4. **Data Security**

a. Company will store and process District Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in NIST Cybersecurity Framework, to secure such data from unauthorized access, disclosure, alteration, and use. Company shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement. Without limiting the foregoing and unless expressly agreed to the contrary in writing, Company warrants that all electronic District Data will be encrypted in transmission and in storage using SSL (Secure Sockets Layer) and stored at no less than 128-bit level encryption.

b. Upon request, Company will provide District a certification indicating that an independent vulnerability or risk assessment of the Company's data security program has occurred.

#### 5. **Security Breach**

a. *Response.* Immediately upon becoming aware of a Security Breach, or of circumstances that have or are likely to have resulted in unauthorized access to, or disclosure of, or use of District Data; Company will notify the District, fully investigate the incident, and cooperate fully with the District's investigation of and response to the incident. Except as otherwise required by law, Company will not provide notice of the incident directly to individuals whose PII was involved, regulatory agencies, or other entities, without prior written permission from the District.

b. *Liability.* In addition to any other remedies available to the District under law or equity, Company will reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused in whole or in part by Company or subcontractors, including but not limited to providing notification to individuals whose PII was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the PII exposed during the breach could be used to commit financial

identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the District as a result of the Security Breach.

## **6. Response to Legal Orders, Demands or Requests for Data**

a. Except as otherwise expressly prohibited by law, Company will immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Company seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

b. If the District receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Tennessee Public Records Act, TCA § 10-7-503), or request seeking District Data maintained by Company (including parent request under FERPA), the District will promptly notify Company and Company will promptly supply the District with copies of the District Data for the District to respond.

## **7. Data Transfer Upon Termination or Expiration**

Upon termination or expiration of this Agreement, Company will ensure that all District Data are securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within a reasonable period of time, and without significant interruption in service. Company shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. In the event that the District requests destruction of its data, Company agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Company might have transferred District Data. The Company agrees to provide documentation of data destruction to the District.

## **8. Audits**

The District reserves the right in its sole discretion to perform audits of Company at the

District's expense to ensure compliance with the terms of this Agreement. The Company shall reasonably cooperate in the performance of such audits.

**9. No End User Agreements.**

This Agreement is the entire agreement between the District (including District employees and other End Users) and the Company. In the event that the Company enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with District employees or other End Users, such agreement shall be null, void and without effect, and the terms of this Agreement shall apply.

**10. Termination.**

This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement between the Parties.

**11. Survival**

The Company's obligations under Section 7 shall survive termination of this Agreement until all District Data has been returned or Securely Destroyed.

**12. Advertisement**

Any and all forms of advertisements, directed towards children, parents, guardians or District employees, as a result of this Agreement, shall be strictly prohibited, unless the District has provided advance written consent.

**13. Governing Law**

This Agreement shall be governed and construed in accordance with the laws of Tennessee, excluding its choice of law rules. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the federal court located in Tennessee or the state court located in Washington County, Tennessee.

**14. Immunities**

The District retains all of its rights and immunities under the Tennessee Governmental Tort Immunity Act, (T.C.A. § 29-20-101 et seq.),

**15. No Assignment**

Company shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of the District.

*[THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT  
BLANK]*



IN WITNESS WHEREOF, the parties have executed this Addendum contemporaneously with the Agreement.

JOHNSON CITY SCHOOL DISTRICT

By \_\_\_\_\_

\_\_\_\_\_  
Title

COMPANY

By: \_\_\_\_\_

Legal Name of Company

\_\_\_\_\_  
FEIN

\_\_\_\_\_  
Signature of Authorized Officer

\_\_\_\_\_  
Printed Name & Title of Authorized Officer

Date: \_\_\_\_\_

Corporations:

(A corporate attestation is required.) Attest (Seal)

By: \_\_\_\_\_

(Corporate Secretary or Equivalent)

(Place corporate seal here, if available.)