

Instructions for Network Evaluation Form Submission

Please follow the steps below to complete and submit the **Network Evaluation Form** to the CPSB Technology Network Operations Department. The form must be submitted for new and existing software/services used with **student personally identifiable information (PII)**.

1. The individual responsible for initiating the purchase of the software/service must fill in the school/department information on the Network Evaluation Form. Do NOT complete this for free services; it is best to keep data anonymous!
2. The vendor/company representative must supply the technical specifications requested on the form. It is the responsibility of CPSB employee seeking to purchase the software/services to work with the Vendor/Company representative in completing the form.
3. Vendor/company must sign the attached addendum to verify compliance under Act 837*. Vendors/companies with questions or concerns regarding the addendum should contact wilfred.bourne@cpsb.org. Technical questions should be directed to Michael.franks@cpsb.org.
4. Submit a Tech Help ticket attaching the the completed form and signed addendum to Network Evaluation/PII workspace. Must be signed by vendor/company before sending in for review.
5. The signature required for the CPSB authorized representative is either:
 - a. the superintendent for services purchased with district funds, or
 - b. the school principal for services purchased with school activity funds.

Once the proper documentation is submitted, the evaluation process may take up to 10 business days to complete which the originator will then be notified. Kirby Smith will acquire the superintendent's signature for approval (district funds) or the principal will sign for school activity funds for Kirby to post approval to the website for completion of the process.

***If the vendor/company cannot or will not verify compliance under Act 837, the service cannot be used with student PII without parental consent.**

Building Foundations for the Future

PRIVACY ADDENDUM

This Privacy Addendum (hereinafter "Addendum") to the Agreement between the parties dated 8-17-15 (hereinafter "Agreement") is entered into by and between the Calcasieu Parish School Board (hereinafter "School Board") and Dorian Business Systems, Inc. (hereinafter "Vendor"). This Addendum is effective as of the 17 day of August, 2015.

The State of Louisiana recently enacted new laws governing the collection, disclosure and use of students' personally identifiable information. The new laws require that any contracts between a school system and a third-party who is entrusted with personally identifiable information of any student contain the statutorily prescribed minimum elements regarding the use of student personally identifiable information (hereinafter "PII"). Vendor agrees to comply with those new laws which are now designated La. R.S. 17:3914, as amended, particularly subsection "F" thereto, and to protect the privacy of student data and PII.

Vendor agrees to protect student information in a manner that allows access to student information, including PII, only by those individuals who are authorized by the Agreement or Addendum to access said information. Personally identifiable information must be protected by appropriate security measures, including, but not limited to, the use of user names, secure passwords, encryption, security questions, and other similar measures. Vendor's network must maintain a high level of electronic protection to ensure the integrity of sensitive information and to prevent unauthorized access in these systems. The Vendor agrees to perform regular reviews of its protection methods and perform system auditing to maintain protection of its systems. Vendor agrees to maintain systems secure from unauthorized access that are patched, up to date, and have all appropriate security updates installed.

To ensure that the only individuals and entities who can access and/or receive student data are those that have been specifically authorized under the Agreement to access and/or receive personally identifiable student data, Vendor shall implement various forms of authentication to identify the specific individual who is accessing or has accessed the information. Vendor must individually determine the level of security that will provide the statutorily required level of protection for the student data it maintains. Vendor shall not allow any individual or entity unauthenticated access to confidential personally identifiable student records or data at any time. Only those individuals whose job duties directly involve fulfillment of the terms of the Agreement or this Addendum, and who are in a "need to know" position, shall be permitted to access PII or student data. Vendor shall provide School Board, upon request, with identities and positions of those persons who are authorized to access PII under the Agreement or the Addendum.

Vendor shall implement appropriate measures to ensure the confidentiality and security of personally identifiable information, protect against any unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to the School Board or any individual identified by the data.

Vendor agrees that any and all personally identifiable student data will be stored, processed, and maintained in a secure location and solely on designated servers. No School Board data, at any time, will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium

is in use as part of the vendor's designated backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the United States unless specifically agreed to in writing by the School Board.

Vendor agrees that any and all data obtained from the School Board shall be used expressly and solely for the purposes enumerated in the Agreement. Data shall not be distributed, used, or shared for any other purpose. As required by Federal and State law, Vendor further agrees that no data of any kind shall be revealed, transmitted, exchanged, or otherwise passed to other vendors or parties. Except as specifically permitted by the terms of the Agreement, Vendor shall not sell, transfer, share, or process any student data for any commercial, advertising, or marketing purpose.

Vendor shall develop a policy for the protection and storage of audit logs. The policy shall require the storing of audit logs and records on a server separate from the system that generates the audit trail. Vendor must restrict access to audit logs to prevent tampering or altering of audit data. Retention of audit trails shall be based on a schedule determined after consultation with operational, technical, risk management, and legal staff.

Vendor is permitted to disclose PII and student data to its employees, authorized subcontractors, agents, consultants and auditors on a need to know basis only, provided that all such subcontractors, agents, consultants, and auditors have written confidentiality obligations to Vendor and the School Board consistent with the terms of this Addendum. The confidentiality obligations shall survive termination of any agreement with Vendor for so long as the information remains confidential, whichever is longer, and will inure to the benefit of the School Board.

Vendor acknowledges and agrees that unauthorized disclosure or use of protected information may irreparably damage the School Board in such a way that adequate compensation could not be obtained solely in monetary damages. Accordingly, the School Board shall have the right to seek injunctive relief restraining the actual or threatened unauthorized disclosure or use of any protected information, in addition to any other remedy otherwise available (including reasonable attorney fees). Vendor hereby waives the posting of a bond by School Board with respect to any action for injunctive relief. Vendor further grants the School Board the right, but not the obligation, to enforce these provisions by suit in Calcasieu Parish, Louisiana, in Vendor's name against any of Vendor's employees, officers, board members, owners, representatives, agents, contractors, and subcontractors.

Vendor shall establish, implement, and provide to School Board evidence thereof, a clear data breach response plan outlining organizational policies and procedures for addressing a potential breach. Vendor's response plan shall require prompt response for minimizing the risk of any further data loss and of any negative consequences of the breach, including potential harm to affected individuals. A data breach is any instance in which there is an unauthorized or unlawful release or access of personally identifiable information or other information not suitable for public release. This definition applies regardless of whether Vendor stores and manages the data directly or through a contractor, such as a cloud service provider.

Vendor agrees to comply with the requirements of La. R.S. 51:3071 *et seq.* (Louisiana Database Breach Notification Law) as well as any other applicable laws regarding notification of individuals of data breaches,

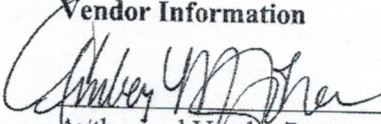
and to provide notification to individuals in the event of unauthorized access to or release of personally identifiable information or other similar event. In the event of a data breach, breach of any of the Vendor's security obligations hereunder, or other event requiring notification under applicable law, Vendor agrees to notify the School Board immediately and assume responsibility for informing all individuals entitled to notice under applicable law, and to indemnify, hold harmless and defend the School Board and its employees from and against any and all claims, damages, or causes of action related to the unauthorized access and/or release.

In accordance with applicable state and federal law, Vendor agrees that auditors from any state, federal, or other agency, as well as auditors so designated by the School Board, shall have the option to audit Vendor's service under the Addendum and the Agreement, including but not limited to privacy and security audits. Records pertaining to the service shall be made available to auditors and the School Board when requested.

Vendor agrees that if the original Contract is terminated or if the original Contract expires, Vendor shall return all data obtained in the performance of its work under the Agreement or the Addendum to the School Board in a useable electronic format. Vendor further agrees to thereafter erase, destroy, and render unreadable all data, in its possession or in the possession of persons and entities with whom it has contracted for the performance of obligations under the Agreement or Addendum, in its entirety in a manner that prevents its physical reconstruction through the use of available file restoration utilities. Vendor shall certify in writing that these actions have been completed within 30 days of the termination of the Contract or within seven (7) days from receipt of any request by the School Board, whichever comes first.

The terms of this Addendum shall supplement and supersede any conflicting terms or conditions of the Agreement between the Parties. Subject to the foregoing, the terms of the original Agreement shall remain in full force and effect.

Vendor Information


Authorized Vendor Representative Signature


Amber Johann
Authorized Representative Name (Print)

Office Manager
Title

Dorian Business Systems Inc
Vendor

8-17-15
Date

CALCASIEU PARISH SCHOOL BOARD


Authorized CPSB Representative Signature

Robert Barrentine
Authorized Representative Name (Print)

Principal
Title

CALCASIEU PARISH SCHOOL

8/21/15
Date

Network Software, Server, Device or Service Evaluation Form

Schools or departments seeking to purchase any software, server, device or service (technology) that will use the CPSB network or be used on a CPSB device must submit this Evaluation Form to the Technology Network Operations Department to determine network and technical compatibility. **Student personally identifiable information (PII) cannot be shared with external entities unless in compliance with ACT 837 and ACT 677.** In order to evaluate and approve the purchase, the following information should be provided by the vendor; this entire form and addendum submitted as a ticket to Tech Help, Network Evaluation / PII (Privacy Addendum).

To be completed by school/department:

School/Department: Sulphur High School

Date: 8/10/15

School/Department Contact: Tim McMillen

Item(s) to be purchased: Charms Office Assistant

Description of providing vendor/company/service: Band management program

How will the item be utilized by the district/school? manage schedule, student accounts, parent comm

Funds used: ☐ CPSB funds ☒ School activity funds

To be completed by vendor/company:

A. Server Information

| | | | |
|--|-----|---------------|----------------|
| 1. Will a server be needed for the network application? (If NO, skip to question 2) | Yes | No | N/A |
| a. Will the application require a dedicated server? | Yes | No | N/A |
| b. Will the brand of the dedicated server be Dell or HP? | Yes | No | N/A |
| c. Will the dedicated server operating system be Windows 2008 R2 / 2012? | Yes | No | N/A |
| d. If an existing server will be used, indicate which one here and attach the hardware specs that the server must have in order to run the application: | | | |
| | | | |
| e. Will a multi-year server contract for application support be purchased for the product? | Yes | No | N/A |
| f. Will the vendor require administrator access to the server to maintain it? | Yes | No | N/A |
| 2. If a service contract for support is not purchased, please write the name(s) of the CPSB staff that will be responsible for maintaining and troubleshooting any application problems. | | | |
| | | | |
| 3. Will the application have a database component requiring data entry? | Yes | No | N/A |
| a. Please write the name(s) of the CPSB staff that will be entering data and maintaining the database. | | | |
| | | | |
| 4. If user authentication is needed, is the application Microsoft Active Directory/LDAP compliant? | Yes | No | N/A |

5. If the application is not Microsoft Active Directory/LDAP compliant, please write the name(s) of the CPSB staff that will be entering user names and passwords and maintaining access control database. Tim McMillen

B. Workstation Client Information

| | | | |
|--|-----|----|-----|
| 1. Does the workstation require a client be installed to access the application? | Yes | No | N/A |
| a. Can the client be installed on the workstation by the end user? | Yes | No | N/A |
| b. Does the client software write to the workstation's registry? | Yes | No | N/A |

C. Workstation Browser Information

| | | | |
|--|-----|----|-----|
| 1. Does the workstation require a browser to access the application? | Yes | No | N/A |
| a. List all compatible browsers and versions that are compatible with this application: Explorer, Firefox, Chrome, Safari | | | |
| b. Will any browser-plug-ins need to be installed for the application to work? | Yes | No | N/A |
| c. Can the required browser plug-in be installed by the end user? | Yes | No | N/A |
| d. Will JAVA be needed on the browser for the software to work? | Yes | No | N/A |
| e. If JAVA is needed, will it work on the latest version? | Yes | No | N/A |

D. Workstation Bandwidth Information

| | | | |
|--|-----|----|-----|
| 1. Will the application be used only on the LAN at a single site? | Yes | No | N/A |
| 2. Will the application be sending data within the district WAN? | Yes | No | N/A |
| 3. Will the application be sending back and forth to the Internet? | Yes | No | N/A |
| 4. If the application will be accessing the Internet, are certain ports required to be open? | Yes | No | N/A |
| a. If ports are required to be opened, list the ports here: | | | |
| 5. Enter the approximate number of workstations that will be accessing the application: 3 | | | |
| 6. Enter the required network bandwidth needed by each workstation for the application: Very little | | | |

E. Wireless Networking Information

| | | | |
|---|-----|----|-----|
| 1. Does the application utilize wireless networking? | Yes | No | N/A |
| 2. Does the server/device have its own wireless access point? | Yes | No | N/A |
| 3. If the device has its own access point, is it Radius compliant? | Yes | No | N/A |
| 4. Will workstations access the application using wireless technology? | Yes | No | N/A |
| 5. Are there existing, approved CPSB access points in place for workstations? | Yes | No | N/A |
| 6. What are the wireless bandwidth requirements for workstations access the application: Charms is strictly web based. No special clients utilized. So in that way, yes they will use wireless if the computer is. | | | |

F. Staff/Student Information

| | | | |
|---|-----|----|-----|
| 1. Will this application require student/staff information for use with the application? If NO, Skip to question 2. | Yes | No | N/A |
| If YES, the following information is required from the Vendor. Please provide documented company policy. | | | |
| a. Company guidelines for authorizing access to the application. | | | |
| b. Company privacy compliance standards. | | | |

| | |
|--|--|
| <p>c. Must be in compliance with Louisiana ACT 837 and ACT 677 for use with student information. Must sign attached addendum to verify compliance. The agreement is not required for use with staff information, only students.</p> <p>d. Availability and frequency of privacy and security audits for company.</p> <p>e. Breach planning, notification and remediation procedures for company.</p> <p style="padding-left: 40px;">All data breach notifications should be sent to Dr. Sheryl Abshire, CPSB CTO at sheryl.abshire@cpsb.org within 48 hours of knowledge of data breach.</p> <p>f. Company information storage, retention, and disposition policies.</p> | |
| 2. List all options available for data integration: | |
| 3. List the CPSB staff that will be responsible for maintaining data integration: | |
| <p>4. Complete listing of student information used with the application:</p> <p>Name, Address, Phone, Email, Height (for uniform measurements), Age, Birthdate, CPSB student ID number, Class information, student account info (band fees, fundraising, etc).</p> | |

Application/Device Demonstration Requirement

If the application/device meets the initial requirements, a working model of the product must be made available to the Technology Department for final testing for compatibility. The applicant and vendor should be ready to provide such resources when requested as part of this process.

Additional Information

If the software, server, device or service is not addressed by the questions above or if there is additional information you would like to include, please write information below or attach it to this form.

Vendor Contact Information

Vendor Name: Dorian Business Systems

Vendor Contact Person: Michael baker

Phone: 972-485-1912 Fax: 972-272-3927

Vendor Website: <https://www.charmsoffice.com>

Vendor Email Address: charmsadmin@charmsmusic.com

FOR QUESTIONS, PLEASE CONTACT THE CSPB TECHNOLOGY OPERATIONS AND SUPPORT AT (337) 217-4357 OR EMAIL michael.franks@cpsb.org.