This Privacy Addendum (hereinafter "Addendum") to the Agreement between the parties dated December 18, 2015 (hereinafter "Agreement") is entered into by and between the Calcasieu Parish School Board (hereinafter "School Board") and Tyler Technologies, Inc. (hereinafter "Vendor"). This Addendum is effective as of the 18th day of APRIL, 2016.

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"). To the extent applicable and to the extent which such measures are within Vendor's control, 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 internal network containing any School Board PII 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 internal systems containing PII 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 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 with regard to School Board PII 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 to which Vendor has been provided access and in Vendor's possession 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 by Vendor, 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

TJH