

BrightBytes, Inc. Data Sharing Agreement

This Data Sharing Agreement ("Agreement") is between the the **Board of Education of River Forest Public Schools District 90 ("Customer")** and BrightBytes, Inc., a Delaware corporation ("**BrightBytes**"), to address data privacy and security relating to student data Customer shares with BrightBytes in connection with the the Applications (as defined below) provided to Customer.

1. **Student Data.** BrightBytes will provide its Technology & Learning Module, Early Warning Module and Intervention Management Module (the "Applications"), which are institutional services and functions, to Customer. In connection with providing the Applications, BrightBytes will obtain Student Data (as defined below) from Customer. Customer authorizes BrightBytes to collect, use and process Student Data (as defined below) for the purpose of providing the Applications as provided under this Agreement. "**Student Data**" is any personal information (in any format) that is directly or indirectly related to an identifiable current or former student that is maintained by Customer or related entity or organization, or by us on Customer's behalf. To the extent that U.S. law applies, Student Data may include "educational records" as defined in the Family Educational Rights and Privacy Act ("**FERPA**"), 20 U.S.C. § 1232(g).
2. **Confidentiality.** BrightBytes agrees to treat Student Data as confidential and not to share it with third parties except as authorized in this Agreement. BrightBytes will only collect Student Data as necessary to fulfill its obligations under this Agreement.
3. **BrightBytes's Access.** Customer authorizes BrightBytes to access or collect Student Data and shall facilitate a reasonable method for BrightBytes to access the information stored in its student information systems ("**SIS**"), learning management system ("**LMS**") or other data repository, or receive Student Data or other information via SIS, Secure File Transfer Protocol ("**SFTP**"), or other secure transfer method. BrightBytes shall access and process Student Data solely for the purposes of providing the Applications and related services as an outsourced institutional function pursuant to FERPA 34 CFR Part 99.31(a)(1). Customer represents and warrants that it has the requisite authority to agree to this Agreement and to provide Student Data to BrightBytes. As between BrightBytes and Customer, Customer owns all right, title, and interest to all Student Data provided or otherwise made available to BrightBytes, and BrightBytes does not own, control, or license such Student Data, except so as to provide the Applications and related services described herein.
4. **Student Data Consents and Authority.** Customer represents and warrants that it has the authority to provide Student Data to BrightBytes for the purpose of providing the Applications as authorized herein. Both parties agree to uphold their responsibilities under all federal and State laws and regulations governing the privacy of Student Data, including, without limitation, in the U.S. the Family Educational Rights and Privacy Act ("**FERPA**"), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy and Protection Act ("**COPPA**"), as applicable. BrightBytes relies on each customer to obtain and provide appropriate consent and disclosures, if necessary, for BrightBytes to collect any Student Data, including the collection of Student Data directly from students under 13, as permitted under COPPA.
5. **Use of Student Data.** By submitting Student Data or other information to BrightBytes, Customer expressly grants, and represents and warrants that it has all rights necessary to grant, to BrightBytes a limited, non-exclusive, license during the Term (as defined below) to use, transmit, distribute, modify, reproduce, display, and store the Student Data solely for the purposes of providing the Applications as contemplated by this Agreement. For clarity and without limitation, BrightBytes shall not use Student Data to engage in targeted advertising.
6. **Use of Anonymized Data.** You agree that BrightBytes may use de-identified data derived from Student Data for product development, research or other purposes, including, but not limited to, operating, analyzing, improving, developing or marketing the Applications, the Clarity Platform and related services. De-identified data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. BrightBytes agrees not

to attempt to re-identify de-identified data and not transfer de-identified data to any party unless that party agrees not to attempt re-identification.”

7. **Third-Party Access.** By submitting Student Data to BrightBytes, you consent to allow BrightBytes to provide access to Student Data to its employees and to certain third party service providers that have a legitimate need to access such information in connection with their responsibilities in providing the Applications and related services. BrightBytes and its employees, subcontractors, service providers, or agents involved in the handling, transmittal, and processing of Student Data will be required to maintain the confidentiality of such data that includes personally identifiable information. BrightBytes represents and warrants that all third parties with whom Student Data is shared will be subject to the terms of this Agreement. BrightBytes will maintain access log(s) that record all disclosures of or third party access to Student Data within its possession, and will provide copies of an access log(s) to Customer upon request.
8. **Data Retention and Deletion Requests.** Customer may request the deletion or retrieval of Student Data in BrightBytes’s possession or in the possession of any third parties with whom BrightBytes has shared Student Data by providing such a request in writing, which request BrightBytes shall then comply with in a commercially reasonable time not to exceed (7) days. If Customer requests that BrightBytes retrieve Student Data, BrightBytes will provide Customer with a copy of all Student Data that was processed during the Term (as defined below). For clarity, BrightBytes will continue to maintain a copy of such data for our records until the end of the Term (as defined below) plus 7 days to allow for a request for retrieval as provided below or until we receive a deletion request. BrightBytes is not required to delete or provide to you any Student Data that has been de-identified, anonymized and/or aggregated, or any data that has been derived from Student Data, so long as the data is maintained in a form, which could not reasonably identify any particular school, educational entity, or individual. Upon termination of this Agreement, BrightBytes will automatically delete or de-identify all Student Data within (7) days unless Customer submits a request to retrieve such data within that time frame.
9. **Data Localization.** You acknowledge and agree that BrightBytes will store and process Student Data in various data centers in the U.S. Student Data shall remain in U.S. and all third party providers must be bound by terms of this Agreement. You also acknowledge that, subject to this Agreement and to the extent permitted by Law, Student Data may be accessed and processed by our affiliates’ or our third party service providers’ personnel and you hereby authorize such access and processing. BrightBytes agrees to provide the names of any affiliates and third party service providers to Customer upon request. BrightBytes warrants and agrees that all affiliates and third party service providers who have access to Student Data will be subject to the terms of this Agreement. Customer warrants and agrees that it has the requisite authority for BrightBytes to process Student Data in the U.S..
10. **Data Security.** We have implemented commercially reasonable administrative, physical and technical safeguards designed to secure Student Data from unauthorized access, disclosure, or use, which could include data encryption, firewalls, physical access controls to buildings and files. We comply with industry best practices for data safeguards and security. We have policies and procedures in place to limit access to our systems to only those employees and trusted third parties that have a need-to-know basis based on specific job function or role. In the event we have a reasonable, good faith belief that an unauthorized party has gained access to or been disclosed personally identifiable Student Data we have collected or received through the Applications, BrightBytes will promptly notify you within three (3) days and will use reasonable efforts to cooperate with your investigation of the incident; and if such incident triggers any third party notice requirements under applicable laws, you agree that as the owner of the Student Data, you will be responsible for the timing, content, cost and method of any such notice and compliance with such laws.
11. **Change of Control.** By submitting Student Data to BrightBytes, you consent to allow BrightBytes to transfer Student Data to a new provider in the event that BrightBytes sells, divests or transfers the business or a portion of the business, provided that the new provider has agreed to data privacy standards no less stringent than those set forth in this Agreement. We may also transfer personal information – under the same conditions – in the course of mergers, acquisitions, bankruptcies, dissolutions, reorganizations, liquidations, similar transactions or proceedings involving all or a portion of our business. [In either case we will provide

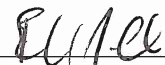

you with notice and an opportunity to opt-out of the transfer of Student Data by deleting your Student Data information and terminating this Agreement.]

12. **Precedence:** In the event of any conflict or inconsistency between the terms of this Agreement and the terms of any other agreement, term of service and/or policy relative to the relationship between the parties hereto, including, without limitation, the BrightBytes' Terms of Service (<http://www.brightbytes.net/privacy-policy-1/>) (the "TOS"), the terms of this Agreement will control. Without limitation, the following terms control despite inconsistency with the TOS
- a. Notice: BrightBytes reserves the right to make modifications to its TOS and will provide prompt notice of these changes, provided, however, that, as noted above, in the event of any conflict or inconsistency between the terms of this Agreement and the TOS, the terms of this Agreement will control.
 - b. Indirect Damages Waiver: Except with respect to liability arising from BrightBytes' own negligence or willful misconduct, BrightBytes and its licensors shall not be liable to you for indirect, incidental, consequential, special, or exemplary damages such as, but not limited to, loss of revenue, data profits, goodwill, or other economic advantage, even if BrightBytes has been previously advised of the possibility of such damages. For the avoidance of doubt, in no event will BrightBytes or its licensors be liable to anyone for any such damages arising out of, or in any way connected with the service or any materials or services, including but not limited to the use or inability to use the service or any content obtained from or through the service.
 - c. Liability Cap: BrightBytes' aggregate liability is capped at amounts equaling the value of the services and licenses that BrightBytes provides in the twelve (12) month period immediately proceeding the event giving rise to such claim under the Technology & Learning module and this Agreement.
 - d. Indemnification: The Customer will only be liable to BrightBytes for damages caused by its negligence and willful misconduct.
 - e. Class Action/Jury Trial: The Customer and BrightBytes do not waive their rights for a trial by Jury or to participate in a class action, collective action, private attorney general action, or other representative proceeding of any kind.

13. **Payment:** The Customer has access to the Applications through an agreement between BrightBytes and West Suburban Cook (West 40). No additional payment is required from Customer for the Applications.

14. **Term and Termination:** The term of this Agreement shall commence upon Customer's first access of any of the Applications and shall end upon the termination of this Agreement pursuant to the terms hereof (the "Term"). Either party shall have the right to terminate this Agreement for any reason or no reason at all by providing the other party at least 30 days prior written notice. The rights and obligations of both parties that should, by their nature or terms, survive termination of this Agreement shall so survive.

This Agreement is signed by duly authorized representatives of the parties and is effective as of the date last signed below.

| | |
|---|--|
| Accepted and agreed to by: | Accepted and agreed to by: |
| CUSTOMER | BRIGHTBYTES, INC |
| Signature: <u></u> | Signature: <u></u> |
| Print Name: <u>EDWARD J. CONDON</u> | Print Name: <u>Giuseppe Basili (Mar 23, 2017)</u> |
| Print Title: <u>SUPERINTENDENT</u> | Print Title: <u>Giuseppe Basili</u> |
| Date: <u>3/24/17</u> | Print Title: <u>Chief Revenue Officer</u> |
| | Date: <u>Mar 23, 2017</u> |