Teacher Created Materials Student Data Policy

This policy applies to all educational institutions (hereinafter referred to as "Licensee") who will collect and store individual student data on a Data Management System set up or administered by Teacher Created Materials, Inc. ("Licensor"). By using the Licensor's Data Management System, you are implicitly agreeing to these privacy practices and agree to accept and be bound by the responsibilities outlined in this policy statement.

Purposes of Data Entry: It is up to the Licensee to control what student data is entered on Licensor's Data Management System. Student data entered on Licensor's Data Management System should be limited to information that is directly relevant to the legitimate educational purpose of improving student performance. Licensor will not ask Licensee to enter, and Licensee is hereby instructed NOT to enter, any data about students that is not directly relevant to the legitimate educational purpose of improving student performance.

A student login is required to be created for each student. Additional data, not specific to the student, is also required to complete system setup, including the teacher first and last name, and the class name. Student demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data and is obtained only with written permission from your educational institution.

Use, Disclosure, and Storage: Licensor will use the student data solely to provide services to the Licensee. Licensor agrees to delete any student data Licensee instructs Licensor to delete. Licensee agrees to utilize student data solely for legitimate educational purposes and agrees to not disclose or otherwise use any student data entered on Licensor's Data Management System for any purposes other than allowed under this Agreement.

Licensor will only disclose student data to authorized employees or representatives of the Licensee, and will not knowingly disclose the student data to any third person without express written authorization from Licensee. When, at the request of the Licensee, Licensor acquires assessment or other information, including personally identifiable student data, from a third party source, Licensor agrees to treat any such information with the same confidentiality and security safeguards as though it were provided directly by the Licensee. Additional agreements may be required by the third party to authorize transmission of data to Licensor.

Licensee may from time to time request that Licensor provide student data to third parties of Licensee's choosing. Licensor will do so only after obtaining written authorization, which acknowledges that Licensor is providing that data as Licensee's agent and that once the data is received by the third party, Licensor no longer has any control or responsibility over the use or disposition of the data.

Licensor may use aggregated data for research, product development, and marketing purposes. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, Licensor will not use personally identifiable student data for any research, product development, or marketing purposes

In the event that Licensor wishes, from time to time, to release aggregated data that

identifies Licensee by name, Licensor will gain authorization from Licensee for such usage prior to release or publication.

Data Quality: Licensee is responsible for keeping Licensee's student data on the site accurate, complete and up-to-date. If Licensee recognizes that student data is inaccurate, incomplete, or out-of-date, Licensee is responsible for correcting student data directly in Licensor's Data Management System. For assistance, or if you experience difficulties making corrections to student data, please feel free to contact Licensor's Customer Service department for help.

Security Safeguards: Licensor is committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from both Licensor and Licensee. Licensor will implement reasonable and appropriate safeguards when collecting student data from Licensee and when storing that student data in Licensor's database. Licensee agrees to observe Licensor security safeguards and exercise reasonable caution when using Licensor's Data Management System.

Specific institutional and technological security safeguards include:

1. Licensor will restrict access to the Data Management System to only those Licensor employees who are authorized to handle student data.
2. Only employees and representatives authorized by the Licensee as school officials are permitted access to the Licensor's Data Management System. The Data Management System will provide the following safeguards, which the Licensee agreed to enforce: a teacher will only be able to see data for his/her class; a Principal, Coach, or other authorized School User will be able to view all data at a given school; an authorized educational institution-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the educational institution.
3. Each Licensee authorized user will be given a Username and Password, valid only for the duration of the license. Licensee must safeguard all Usernames and Passwords, and not permit any unauthorized access to student data entered or kept in Licensor's Data Management System. Upon written request by the Licensee, Licensor will destroy any student data for educational institutions who no longer participate in a Licensor program. Licensor will provide written verification that the data has been destroyed as requested.
4. If an educational institution has not used the Data Management System for a period of ten years, Licensor may destroy student data pertaining to that educational institution, unless the educational institution requests the records be kept.
5. Licensor agrees to utilize industry standard server and network hardware and software to protect data from unauthorized access or disclosure.

By accessing and using the Data Management System, you consent to these privacy practices and agree to accept the responsibilities outlined in this policy.