RATINGS SYSTEM INC. DATA AND PRIVACY POLICY

WHEREAS, Ratings System Inc. (the "Provider") is the owner and sole source provider of certain proprietary computer software known as EdCredible that is used to evaluate, rate and review products, services, instructional materials, state standards and test item specifications utilized in Education (the "Services"); and

WHEREAS, persons within Local Education Agencies, State Education Agencies, parents, community members and other laypeople access Services for the purpose of participating in instructional materials adoptions (the "User"); and

WHEREAS, the Provider and User are collectively known as (the "Parties"); and

WHEREAS, in order to provide the Services, the Provider may receive and the User may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), at 15 U.S.C. 6501-6506 (16 CFR Part 312), and Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and

WHEREAS, the documents and data transferred from User and/or accessed by the Provider in the use of Services are also subject to state privacy laws; and

WHEREAS, this Data And Privacy Policy (the "Privacy Policy") complies with State and Federal statutes and laws; and

WHEREAS, the Parties agree to the terms set forth in this Privacy Policy to ensure that accessing and/or transferring of data is in compliance with state and federal law and Provider Privacy Policy.

NOW THEREFORE, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of Data And Privacy Policy**. For Provider to provide services to the User it may become necessary for the User to share certain User Data related to the User's students, employees, business practices, and/or intellectual property. This agreement describes the responsibilities to protect Data between the User and Provider.

2. **Data to Be Provided**. In order to perform the Services, User shall provide the categories of data including: ***First Name***, ***Last Name***, ***Email***, ***User Role*** (i.e. District Admin, School Admin, Teacher, Parent, etc.) and ***School Name*** (if applicable).

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1 **Data Property of User**. Provider acknowledges that all right, title and interest in any personally identifiable data (PID) provided by or collected by User through the use of Services ("User Data") is, and at all times shall remain, the sole and exclusive property of User, unless otherwise specified in advance to User by Provider.

Provider will not use, sell, distribute, disclose or publish any PID without the express written consent of the User. Except the right to use the User's Data to produce electronic or hard copy reports with PID for the User's exclusive use, this policy does not grant to Provider any rights to PID. **EXCEPT THE RIGHT BY THE USER TO ACCESS AND USE CHARTS AND GRAPHS AND OTHER DATA COLLECTED THROUGH THE USE OF THE SERVICES, PROVIDER STRICTLY PROHIBITS USER DISTRIBUTION OF ANY AND ALL QUANTIFIABLE "RAW" DATA COLLECTED THROUGH SERVICES TO ANY THIRD PARTY FOR ANY COMMERCIAL, NON-COMMERCIAL, RESEARCH-BASED USE OR ANY OTHER USE THAT IS NOT EXPLICITLY AUTHORIZED BY PROVIDER IN WRITING TO ACCESS USER DATA.**

User acknowledges that all right, title, and interest in and to Provider, together with its codes, sequences, derivative works, organization, structure, interfaces, any documentation, data, trade names, trademarks, or other related materials (collectively, the "Provider IP"), is, and at all times shall remain, the sole and exclusive property of Provider. The Provider IP contains trade secrets and proprietary information owned by Provider and is protected by United States copyright laws (and other laws relating to intellectual property). Except the right to use the Services, as expressly provided herein, the Provider does not grant to User any rights to, or patents in, copyrights, database rights, trade secrets, trade names, trademarks (whether registered or unregistered) or other rights or licenses with respect to the Services or the Software.

2 **Non-Administrative User Data Access**. Provider shall respond in a reasonable manner (and no less than 10 business days from the date of request) to the User request for User Data held by the Provider to view or correct as necessary. In the event that a parent, student, layman or any other "Non-administrative User" contacts the Provider to review, obtain or otherwise collect any User Data collected in the Services, the Provider shall refer the Non-administrative User to the designated User Administrator, who will follow the necessary and proper procedures regarding the requested information.

3 **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the User. Provider shall notify the User in advance of a compelled disclosure to a Third Party. The Provider will not use, disclose, compile, transfer, or sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof.

4. **No Unauthorized Use**. Provider shall not use Data for any purpose other than as explicitly specified by the Parties and in a written agreement and/or in accordance with the Privacy Policy.

5. **Subcontractors**. In the event Provider enters into agreements with Subcontractors, Subcontractors performing functions for the Provider Services shall agree to protect Data in a manner consistent with the terms of this Privacy Policy and any written User Agreement.

ARTICLE III: DUTIES OF USER

1. **Provide Data In Compliance With State and Federal Law**. User will allow Provider access to data necessary to perform the services pursuant to any Services Agreement and pursuant to the terms of this Privacy Policy and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this Privacy Policy.

2. **Annual Notification of Rights.** If the User has a policy of disclosing education records under 34 CFR § 99.31 (a) (1), User shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights and determine whether Provider qualifies as a school official.

3. **Reasonable Precautions**. The User shall take reasonable precautions to secure user names, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. The User shall notify Provider promptly of any known or suspected unauthorized access. User will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Parties expect and anticipate that Provider may receive PID in education records from the User only as an incident of service or training that Provider provides to the User during the use of Services. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, state statutes and all other privacy statutes cited in this Privacy Policy.

2. **Authorized Use**. The data shared pursuant to any agreement between the Parties, including persistent unique identifiers, shall be used for no purpose other than the Services stated in any written agreement between the Parties and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not disclose any non-public information and/or PID contained in the User Data, without the express written consent of the User. Provider may collect data in the way of anonymous User "reviews" (feedback) about the Service and/or products reviewed in the Service; and may use anonymous User "review" to generate anonymized aggregate reports specifically for Local Education Agency and State Education Agency Users.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Data to comply with all applicable provisions of this Privacy Policy with respect to the data shared under any written agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or contract with access to User Data.

4. **No Disclosure**. Provider may use aggregate data only for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to User who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any User data that is property of the User. Pursuant to subsection (2) of this Section, Provider may collect and make available anonymous User "reviews" to the Local and/or State Education Agency.

5. **Disposition of Data**. Provider shall dispose of or delete all Data obtained when it is no longer needed for the purpose for which it was obtained and transfer said data to User or User's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Provider is not required to maintain Data obtained under any written agreement beyond the time-period reasonably needed to complete the disposition. Disposition shall include:

    a. (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to User when the Data has been disposed of. Upon receipt of a request from the User, the Provider will immediately provide the User with any specified portion of the Data within ten (10) calendar days of receipt of said request.

    b. **Access to Data**. Provider shall make Data in the possession of the Provider available to the User as soon as reasonably possible, but no later than (10) business days of a request by the User.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below.

   a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Data in accordance with industry best practices. The Provider shall only provide access to Data to employees or Providers that are performing the Services.

   b. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by User.

   c. **Employee Training.** Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide User with contact information of an employee who User may contact if there are any security concerns or questions.

   d. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider hosting is managed by Amazon Web Services and all appropriate security measures shall be in place to maintain the integrity of User Data and Provider Service.

   e. **Periodic Risk Assessment**. Provider conducts periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Provider will promptly modify its security measures as needed based on risk assessment results in order to meet its obligations under this Privacy Policy.

   f. **Backups.** Provider maintains backup copies of Data in case of system failure or any other unforeseen event resulting in loss of Data or any portion thereof.

2. **Data Confidentiality -** Provider implements appropriate measures designed to ensure the confidentiality and security of PID, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to User or an individual identified with the data or information in Provider's custody.

3. **<u>Data Breach</u>**. Provider certifies that it has implemented policies and procedures addressing a potential Security Breach.

   a. Provider complies with all applicable federal and state laws that require notification to individuals, entities, state agencies, or federal agencies in the event of a Security Breach including the State of Florida Database Breach Notification process.

   b. When Provider reasonably suspects and/or becomes aware of a disclosure or security breach concerning any Data covered by any agreement, Provider shall notify User immediately and mitigate the damage of such security breach to the greatest extent possible. Provider agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   c. Provider further agrees that it will provide the notification directly to User and will fully cooperate, and assist as specifically requested by User, with all efforts by the User to notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information listed in subsection (a) above.

   d. The Parties agree that any breach of the privacy and/or confidentiality obligation set forth in the Privacy Policy may, at the User's discretion, result in the User immediately terminating the any written agreement and any other agreement for goods and services with Provider.

ARTICLE VI: MISCELLANEOUS

1. **<u>Term</u>**. The Provider shall be bound by this Privacy Policy for the duration of the Service Agreement or so long as the Provider maintains any Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this Privacy Policy for no less than three (3) years.

2. **<u>Termination</u>**. In the event that either Party seeks to terminate this Privacy Policy, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **<u>Notice</u>**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

4. **<u>Severability</u>**. Any provision of this Privacy Policy that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this

Privacy Policy, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this Privacy Policy or affecting the validity or enforceability of such provision in any other jurisdiction.

5. **Authority**. Provider represents that it is authorized to bind to the terms of this Privacy Policy, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or Providers who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.

6. **Waiver**. Waiver by any party to this Privacy Policy of any breach of any provision of this Privacy Policy or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this Privacy Policy shall not operate as a waiver of such right. All rights and remedies provided for in this Privacy Policy are cumulative. Nothing in this Privacy Policy shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the User, its officers, employees, and agents as a result of the execution of this Privacy Policy or performance of the functions or obligations described herein.

7. **Assignment**. Neither Party may assign their rights, duties, or obligations under this Privacy Policy, either in whole or in part, without the prior written consent of the other party to this Privacy Policy.