DATA PRIVACY POLICY

Level8Creative

LAST UPDATED: OCTOBER 1, 2022

This Data Privacy Policy ("DPP") shall describe Level8Creative, LLC's (the "Provider") data privacy policies and procedures.

PURPOSE OF THE DPP

The Provider may provide a "Local Education Agency", as defined at 34CFR§303.23 ("LEA(s)") with certain digital educational services ("Services") pursuant to services agreements ("Service Agreement"). In order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA 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"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h. In addition, the documents and data transferred from LEAs and created by the Provider's Services may also be subject to various state data practices laws and regulations, as described in the applicable Service Agreement (the "State Laws").

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPP. The purpose of this DPP is to describe the duties and responsibilities to protect data transmitted to Provider from the LEA pursuant to a Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, MGDPA and other applicable State Laws. In performing services requiring access to private records/data on students, the Provider shall be considered a "School Official", as defined in [CITE) with a legitimate educational interest, and performing services otherwise provided by the LEA.

2. Data to Be Provided. The Parties shall indicate the categories of data to be provided in the applicable Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. Data Property of LEA. All LEA data transmitted to the Provider pursuant to the Service Agreement (the "LEA Data") is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such LEA Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original LEA Data. All rights, including all intellectual property rights in and to LEA Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.

2. Parent Access. If required in the Service Agreement, LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review student data in the student's records, correct erroneous information, and procedures for the transfer of student generated content to a personal account, consistent with the functionality of Services. Provider shall respond in a timely manner (and no later than 45 days from the date of receipt of LEA's written request) to the LEA's written request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual

contacts the Provider to review any of the student data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. Separate Account. If student generated content is stored or maintained by the Provider, Provider shall, upon receipt of the written request of the LEA, transfer said Student Generated Content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

4. 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 LEA. Provider shall notify the LEA in advance of a compelled disclosure to a third party unless legally prohibited.

5. Subcontractors. Provider shall enter into written agreements with all third-party contractors performing functions pursuant to the Service Agreement, whereby said contractors agree to protect LEA Data in manner consistent with the terms of this DPP.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA and other applicable State Laws. Provider agrees that any information it creates, collects, receives, stores, uses, or disseminates during the course of its performance, which concerns the personal, financial, or other affairs of the LEA, its employees, students, and parents, relatives, or guardians, shall be kept private and in conformance with all applicable state and federal laws relating to data privacy.

2. Authorized Use. The LEA Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any LEA Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the LEA Data, without the express written consent of the LEA.

3. Employee Obligation. Provider shall require all employees and agents who have access to LEA Data to comply with all applicable provisions of this DPP with respect to the LEA Data shared under a Service Agreement.

4. No Disclosure. Provider maintains the perpetual right to use deidentified data for product development, product functionality and research purposes, as permitted under FERPA. Deidentified data may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications. Provider agrees not to attempt to re-identify de-identified LEA Data and not to transfer de-identified LEA 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 LEA. Provider shall not copy, reproduce or transmit any LEA Data obtained under the

Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement. As used herein, "Deidentified Data" refers to data that does not identify an individual and there is no reasonable basis to believe that the information, either alone or in combination with other data, can be used to identify an individual.

5. Disposition of Data. Upon receipt of LEA's written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all LEA Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Destruction of LEA Data will not include data which has been archived for disaster recovery purposes, which data will be removed from Provider's backup servers over time, in accordance with and consistent with standard industry practice. Any such archived data shall remain fully subject to the confidentiality obligations set forth in the DPP. Upon Provider's receipt of LEA's written request, Provider shall provide written notification to LEA when the LEA Data has been disposed. The duty to dispose of LEA Data shall not extend to any data that has been de-identified or placed in a separate user account, pursuant to the other terms of this DPP. Upon receipt of a written request from the LEA, the Provider will promptly provide the LEA with any specified portion of the LEA Data within 30 calendar days of Provider's receipt of said written request.

a. Partial Disposal During Term of Service Agreement. Throughout the Term of the Service Agreement, LEA may request, in writing, partial disposal of LEA Data obtained under the Service Agreement that LEA reasonably believes, and Provider reasonably agrees, is no longer needed. LEA may also request. in writing, that specific LEA Data be returned to the LEA.

b. Complete Disposal Upon Termination of Service Agreement. Upon Termination of the Service Agreement and upon Provider's receipt of LEA's written request, Provider shall dispose or delete all LEA Data obtained under the Service Agreement.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider maintain commercially reasonable data security measures to protect LEA Data from unauthorized disclosure or use. These measures shall include:

a. Passwords and Employee Access. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to LEA Data. Provider shall only provide access to LEA Data to employees or contractors that are performing the Services. Employees or subcontractors with access to LEA Data shall have signed confidentiality agreements regarding said LEA Data.

b. Destruction of Data. Upon receipt of LEA's written request, Provider shall destroy or delete all LEA Data obtained under the Service Agreement or transfer said data to LEA or LEA's designee.

c. Security Protocols. Provider shall maintain all LEA Data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy,

reproduce, or transmit LEA Data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. Employee Training. The Provider shall provide periodic (no less than annual) security training, to those of its employees who operate or have access to the Provider's computer systems and/or the LEA Data.

e. Mobile Use of LEA Data. Provider shall ensure that any and all mobile devices of any type (including, but not limited to, laptops, tablets, and phones), which are used for access to, storage or analysis of LEA Data by Provider's employees, contractors and/or subcontractors shall be protected by commercially reasonable standard encryption to prevent unauthorized access by third parties.

f. Security Technology. When LEA Data is accessed using a supported web browser, Provider shall employ commercially reasonable measures to protect LEA Data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host LEA Data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

h. Subcontractors Bound. Provider shall enter into written agreements whereby subcontractors agree to secure and protect LEA Data in a manner consistent with the terms of this Article V. Provider shall periodically (no less than annual) conduct or review compliance monitoring and assessments of subcontractors to determine their compliance with this Article.

i. Periodic Risk Assessment. Provider shall conduct digital and physical periodic (no less than annual) risk assessments and remediate any identified material vulnerabilities relating to security or privacy in a timely manner.

j. Compliance Audit. Upon receipt of written request, Provider will provide a written summary of the most recent internal security and compliance audit that Provider has performed on its IT security practices. Provider will perform such internal security and compliance audits in no event less frequently than once per year.

2. Data Breach. In the event that LEA Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding 5 business days. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

iii. If the information is possible to determine at the time the notice is provided, the number of individuals whose data was potentially subject to the breach and either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the LEA Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects commercially reasonable practices that is consistent with applicable federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of LEA Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure LEA Data.