Version 2.0 Agreement Approved: June 2019

# DATA PRIVACY AGREEMENT (DPA)
# FOR TEXAS K-12 INSTITUTIONS

LEA NAME [Box 1]     DATE  [Box 2]

and

## Epic! Creations, Inc.   10-18-2023

OPERATOR NAME [Box 3]     DATE [Box 4]

## Background and Instructions

**History of Agreement-** This agreement has been drafted by the Texas Student Privacy Alliance (TXSPA). The Alliance is a collaborative group of Texas school districts that share common concerns around student and data privacy. The Texas K-12 CTO Council is the organization that sponsors the TXSPA and the TXSPA is the Texas affiliate of the national Student Data Privacy Consortium (SDPC). The SDPC works with other state alliances by helping establish common data privacy agreements unique to the jurisdiction of each state. This Texas agreement was drafted specifically for K-12 education institutions and included broad stakeholder input from Texas school districts, statewide associations such as TASB, TASA, and TASBO, and the Texas Education Agency. The purpose of this agreement is to set standards of both practice and expectations around data privacy such that all parties involved have a common understanding of expectations. This agreement also provides a mechanism (Exhibit E- General Offer of Terms) that would allow an Operator to extend the ability of other Texas school districts to be covered under the terms of the agreement should an Operator sign Exhibit E. This mechanism is intended to create efficiencies for both Operators and LEAs and generally enhance privacy practices and expectations for K-12 institutions and for companies providing services to K-12 institutions.

**Instructions for Operators:** This agreement is intended to be provided to an Operator from a LEA. The Operator should fully read the agreement and is requested to complete the below areas of the agreement. Once the Operator accepts the terms of the agreement, the Operator should wet sign the agreement and return it to the LEA. Once the LEA signs the agreement, the LEA should provide a signed copy of the agreement to the Operator.

| Article/Exhibit | Box # | Description |
|---|---|---|
| Cover Page | Box # 3 | Official Name of Operator |
| Cover Page | Box # 4 | Date Signed by Operator |
| Recitals | Box #5 | Contract Title for Service Agreement |
| Recitals | Box #6 | Date of Service Agreement |
| Article 7 | Boxes #7-10 | Operator's designated representative |
| Signature Page | Boxes #15-19 | Authorized Operator's representative signature |
| Exhibit A | Box #25 | Description of services provided |
| Exhibit B | All Applicable Boxes | • Operator notates if data is collected to provide the described services.<br>• Defines the schedule of data required for the Operator to provide the services outlined in Exhibit A |
| Exhibit D | All Applicable Boxes | (Optional Exhibit): Defines deletion or return of data expectations by LEA |

| Exhibit E | All Applicable Boxes | (Optional Exhibit): Operator may, by signing the Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other Subscribing LEA who signs the acceptance in said Exhibit. |
| Exhibit F | Boxes # 25-29 | A list of all Subprocessors used by the Operator to perform functions pursuant to the Service Agreement, list security programs and measures, list Operator's security measures |

**Instructions for LEA and/or Subscribing LEA:** This agreement is intended to be provided to an Operator from a LEA. Upon receiving an executed agreement from an Operator, the LEA should fully review the agreement and if agreeable, should have an authorized LEA contact wet sign the agreement. Once signed by both the Operator and LEA, the LEA should send a copy of the signed agreement to the Operator.

| Article/Exhibit | Box # | Description |
|---|---|---|
| Cover Page | Box # 1 | Official Name of LEA |
| Cover Page | Box #2 | Date Signed by LEA |
| Article 7 | Boxes #11-14 | LEA's designated representative |
| Signature Page | Boxes #20-24 | Authorized LEA representative's signature |
| Exhibit D | All Applicable Boxes | (Optional Exhibit): Defines deletion or return of data expectations by LEA |
| Exhibit E | All Applicable Boxes | (Optional Exhibit) Only to be completed by a Subscribing LEA |

# RECITALS

**WHEREAS,** the Operator has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") according to a contract titled "<u>Epic! Terms of Service</u>"

<center>[Box 5]</center>

and dated <u>10/18/23</u> (tbe "Service Agreement"), and

<center>[Box 6]</center>

**WHEREAS,** in order to provide the Services described in the Service Agreement, the Operator may

receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal 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, and Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

**WHEREAS,** the documents and data transferred from LEAs and created by the Operator's Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

**WHEREAS**, the Operator may, by signing the "General Offer of Privacy Terms", agree to allow other

LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described within, without the need to negotiate terms in a separate DPA.

**NOW THEREFORE,** for good and valuable consideration, the parties agree as follows:

## ARTICLE I: PURPOSE AND SCOPE

**<u>Nature of Services Provided</u>**. The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement

1. **<u>Purpose of DPA</u>**. For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties' responsibilities to protect Data.

2. **<u>Data to Be Provided</u>**. In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.

**<u>DPA Definitions</u>**. The definitions of terms used in this DPA are found in Exhibit C. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement will continue to be the property of and under the control of the LEA. The Operator further

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Ownership of Data**. All Data transmitted to the Operator pursuant to the Service Agreement is and acknowledges and agrees that all copies of such Data transmitted to the Operator, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.

2. **Operator Materials**. Operator retains all right, title and interest in and to any and all of Operator's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Operator Materials"). Operator grants to the LEA a personal, nonexclusive license to use the Operator Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Operator represents that it has all intellectual property rights necessary to enter into and perform its obligations in this DPA and the Service Agreement, warrants to the District that the District will have use of any intellectual property contemplated by the Service Agreement free and clear of claims of any nature by any third Party including, without limitation, copyright or patent infringement claims, and agrees to indemnify the District for any related claims.

3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 28 days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

4. **Data Portability**. Operator shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format.

5. **Third Party Request**. Should a Third Party, including law enforcement or a government entity, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within 1 business day), and to the extent legally permitted, redirect the Third Party to request the data directly from the LEA, notify the LEA of the request, and provide a copy of the request to the LEA. Furthermore, if legally permissible, Operator shall promptly notify the LEA of a subpoena compelling disclosure to a Third Party and provide a copy of the subpoena with sufficient time for the LEA to raise objections to the subpoena. The Operator 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. Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act
(Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.

6. **No Unauthorized Use**. Operator shall use Data only for the purpose of fulfilling its duties and obligations under the Service Agreement and will not share Data with or disclose it to any Third Party without the prior written consent of the LEA, except as required by law or to fulfill its duties and obligations under the Service Agreement.

   **Subprocessors**. All Subprocessors used by the Operator to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to

determine their compliance with this DPA. Subprocessors shall agree to the provisions of the DPA regarding governing law, venue, and jurisdiction.

## ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA as these laws and regulations apply to the contracted services. The LEA shall not be required to provide Data in violation of applicable laws. Operator may not require LEA or users to waive rights under applicable laws in connection with use of the Services.

2. **Consider Operator as School Official.** The Parties agree that Operator is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records. For purposes of the Service Agreement and this DPA, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records

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

4. **Unauthorized Access Notification**. LEA shall notify Operator promptly of any known unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

## ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance**. Operator may receive Personally Identifiable Information ("PII") from the District in the course of fulfilling its duties and obligations under the Service Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA.

2. **Employee Obligation**. Operator shall require all employees and agents who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.

3. **De-identified Information**. De-identified Information may be used by the Operator only for the purposes of development, product improvement, to demonstrate or market product effectiveness, or research as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify De-identified Information and not to transfer De-identified Information 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 who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any De-identified Information or other Data obtained under the Service Agreement except as necessary to fulfill the Service Agreement.

4. **Access To, Return, and Disposition of Data**. Upon written request of LEA, Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to LEA or LEA's designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Operator acknowledges LEA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by LEA. Nothing in the Service Agreement shall authorize Operator to maintain Data obtained under the Service Agreement beyond the time

period reasonably needed to complete the disposition. Disposition shall include (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. Operator shall provide written notification to LEA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" FORM, a sample of this form is attached on Exhibit "D"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within five (5) business days of receipt of said request.

5. **Targeted Advertising Prohibition**. Operator is prohibited from using or selling Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.

(di) **Access to Data**. Operator shall make Data in the possession of the Operator available to the LEA within five (5) business days of a request by the LEA.

## ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Operator 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 Operator are set forth below. Operator shall further detail its security programs and measures in Exhibit F. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access**. Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level consistent with an industry standard agreed upon by LEA (e.g. suggested by Article 4.3 of NIST 800-63-3). Operator shall only provide access to Data to employees or subprocessors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.

   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. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment.

   c. **Employee Training**. The Operator shall provide periodic security training to those of its employees who operate or have access to the system.

   d. **Security Technology**. When the Services are 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. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

   f. **Security Contact**. Operator shall provide the name and contact information of Operator's Security Contact on Exhibit F. The LEA may direct security concerns or questions to the Security Contact.

6

**g. Periodic Risk Assessment**. Operator shall conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA an executive summary of the risk assessment or equivalent report and confirmation of remediation.

**h. Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of any portion of Data.

**i. Audits.** Within 30 days of receiving **a** request from the LEA, and not to exceed one request per year, the LEA may audit the measures outlined in the DPA. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA. The LEA may request an additional audit if a material concern is identified.

**j.** Operator shall have a written incident response plan that reflects best practices and is consistent with
industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of any portion of Data, including PII, and agrees to provide LEA, upon request, an executive summary of the written incident response plan.

2. **Data Breach**. When Operator reasonably suspects and/or becomes aware of an unauthorized disclosure or security breach concerning any Data covered by this Agreement, Operator shall notify the District within 24 hours. The Operator shall take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible. If the incident involves criminal intent, then the Operator will follow direction from the Law Enforcement Agencies involved in the case.
   a. The security breach notification to the LEA shall be written in plain language, and address the following

      1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
      2. A description of the circumstances surrounding the disclosure or breach, including the actual or estimated, time and date of the breach, and Whether the notification was delayed as a result of a law enforcement investigation.

   b. Operator agrees to adhere to all requirements in applicable state and federal law with respect to a Data breach or disclosure, including any required responsibilities and procedures for notification or mitigation
   c. In the event of a breach or unauthorized disclosure, the Operator shall cooperate reasonnably ~~fully~~ with the LEA, including, but not limited to providing appropriate notification to individuals impacted by the breach or disclosure. Operator will reimburse the LEA in full for all costs incurred by the LEA in investigation and remediation of any Security Breach caused in whole or in part by Operator or Operator's subprocessors, including but not limited to costs of providing notification and providing one year's credit monitoring to affected individuals if PII exposed during the breach could be used to commit financial identity theft.
   d. The LEA may immediately terminate the Service Agreement if the LEA determines the Operator has breached a material term of this DPA.
   e. The Operator's obligations under Section 7 shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

## ARTICLE VI- GENERAL OFFER OF PRIVACY TERMS

1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

.

## ARTICLE VII:
## MISCELLANEOUS

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

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Operator shall dispose of all of LEA's Data pursuant to Article IV, section 5.

4. **Priority of Agreements**. This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. 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: The designated representative for the Operator for this Agreement is:

| | | |
|---|---|---|
| First Name: | Norman | [Box 7] |
| Last Name: | Basch | [Box 8] |
| Operator's Company Name: | Epic! Creations, Inc. | [Box 9] |
| Title of Representative: | VP | [Box 10] |

The designated representative for the LEA for this Agreement is:

| | | |
|---|---|---|
| First Name: | | [Box 11] |
| Last Name: | | [Box 12] |
| LEA's Name: | | [Box 13] |
| Title of Representative: | | [Box 14] |

8

6.  **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter and supersedes all prior communications, representations, or agreements, oral or written, by the Parties. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7.  **Severability**. Any provision of this DPA 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 DPA, 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 DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8.  **Governing Law: Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9.  **Authority**. Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors 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.

10. **Waiver**. Waiver by any party to this DPA of any breach of any provision of this DPA 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 DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.

11. **Assignment**. The Parties may not assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other Party except that either party may assign any of its rights and obligations under this DPA without consent in connection with any merger (including without limitation by operation of law), consolidation, reorganization, or sale of all or substantially all of its related assets or similar transaction. This DPA inures to the benefit of and shall be binding on the Parties' permitted assignees, transferees and successors.

[*Signature Page Follows*]

## EXHIBIT " E"

### GENERAL OFFER OF PRIVACY TERMS

**Instructions:** This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit.   The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E  and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

### 1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and

[

and which is dated [    10/18/23    ] to any other LEA ("Subscribing LEA") who accepts  this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the event of:

(1) a material change in the applicable privacy statutes;
(2) a material change in the services and products listed in the Originating Service Agreement;
(3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.
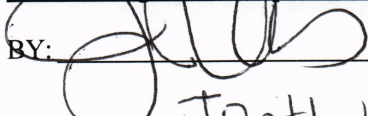
### Operator's Representative:

BY: _Kevin Donahue_
DocuSigned by:
8423705FADCB4F0...

Date: **10/18/23**

Printed Name: **Kevin Donahue**

Title/Position: **Co-Founder**

### 2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

### Subscribing LEA's Representative:

BY: _[signature]_

Date: 12-1-2023

Printed Name: Joette Rios

Title/Position: Digital Learning Coordinator

**IN WITNESS WHEREOF**, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

**Operator's Representative:**

BY: _Kevin Donahue_ [Box 15]    Date: 10/18/23 [Box 16]

8423705FADCB4F0...

Printed Name: Kevin Donahue [Box 17]    Title/Position: Co-Founder [Box 18]

Address for Notice Purposes: privacy@getepic.com [Box 19]

**LEA's Representative**

BY: _____ [Box 20]    Date: _____ [Box 21]

Printed Name: _____ [Box 22]    Title/Position: _____ [Box 23]

Address for Notice Purposes: _____ [Box 24]

*Note: Electronic signature not permitted.*

<u>**EXHIBIT "A"**</u>

DESCRIPTION OF SERVICES

Description :  [Box 25]

 Epic School and Epic School Plus digital product offerings.

**EXHIBIT " B"**

SCHEDULE OF DATA

**Instructions**:  Operator should identify if LEA data is collected to provide the described services.  If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the "Other" category to list the data collected.

☐    We do not collect LEA Data to provide the described services.

■    We do collect LEA Data to provide the described services.

**SCHEDULE OF DATA**

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Application Technology Meta Data | IP Addresses of users, Use of cookies etc. | ☒ |
| | Other application technology meta data-Please specify: | ☐ |
| | | |
| Application Use Statistics | Meta data on user interaction with application- Please specify: | ☒ |
| | | |
| Assessment | Standardized test scores | ☐ |
| | Observation data | ☐ |
| | Other assessment data-Please specify: Teacher Created Quizzes | ☒ |
| | | |
| Attendance | Student school (daily) attendance data | ☐ |
| | Student class attendance data | ☐ |
| | | |
| Communications | Online communications that are captured (emails, blog entries) | ☐ |
| | | |
| Conduct | Conduct or behavioral data | ☐ |
| | | |
| | Date of Birth | ☐ |

| | | |
|---|---|---|
| Demographics | Place of Birth | ☐ |
| | Gender | ☐ |
| | Ethnicity or race | ☐ |
| | Language information (native, preferred or primary language spoken by student) | ☐ |
| | Other demographic information-Please specify: | ☐ |
| Enrollment | Student school enrollment | ☐ |
| | Student grade level | ☒ |
| | Homeroom | ☐ |
| | Guidance counselor | ☐ |
| | Specific curriculum programs | ☐ |
| | Year of graduation | ☐ |
| | Other enrollment information-Please specify: | ☐ |
| | | |
| Parent/Guardian Contact Information | Address | ☐ |
| | Email | ☐ |
| | Phone | ☐ |
| | | |
| Parent/Guardian ID | Parent ID number (created to link parents to students) | ☐ |
| | | |
| Parent/Guardian Name | First and/or Last | ☐ |
| | | |
| Schedule | Student scheduled courses | ☐ |
| | Teacher names | ☒ |
| | | |
| Special Indicator | English language learner information | ☐ |
| | Low income status | ☐ |
| | Medical alerts /health data | ☐ |
| | Student disability information | ☐ |
| | Specialized education services (IEP or 504) | ☐ |
| | Living situations (homeless/foster care) | ☐ |
| | Other indicator information-Please specify: | ☐ |

| Category of Data | Elements | Check if used by your system |
|---|---|---|
| Student Contact Information | Address | ☐ |
| | Email | ☐ |
| | Phone | ☐ |
| | | |
| Student Identifiers | Local (School district) ID number | ☐ |
| | State ID number | ☐ |
| | Vendor/App assigned student ID number | ☐ |
| | Student app username | ☒ |
| | Student app passwords | ☒ |
| | | |
| Student Name | First and/or Last | ☒ |
| | | |
| Student In App Performance | Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) | ☒ |
| | | |
| Student Program Membership | Academic or extracurricular activities a student may belong to or participate in | ☐ |
| | | |
| Student Survey Responses | Student responses to surveys or questionnaires | ☐ |
| | | |
| Student work | Student generated content; writing, pictures etc. | ☐ |
| | Other student work data -Please specify: | ☐ |
| | | |
| Transcript | Student course grades | ☐ |
| | Student course data | ☐ |
| | Student course grades/performance scores | ☐ |
| | Other transcript data -Please specify: | ☐ |
| | Student bus assignment | ☐ |
| | Student pick up and/or drop off location | ☐ |

| | | | |
|---|---|---|---|
| Transportation | Student bus card ID number | | ☐ |
| | Other transportation data -Please specify: | | ☐ |
| | | | |
| Other | Please list each additional data element used, stored or collected through the services defined in Exhibit A | | ☐ |

## EXHIBIT "C"

DEFINITIONS

**HB 2087:** The statutory designation for what is now Texas Education Code Chapter 32 relating to pupil records.

**Data:** Data shall include, but is not limited to, the following: student data, educational records, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

**De-Identified Information (DII):** De-Identified Information is Data subjected to a process by which any Personally Identifiable Information ("PII") is removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual or information about them, and cannot be reasonably re-identified.

**Data Destruction:** Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased, de-identified or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

**NIST 800-63-3**: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

**Personally Identifiable Information (PII):** The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

**Pupil-Generated Content:** The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

**Subscribing LEA:** A LEA that was not party to the original Services Agreement and who accepts the Operator's General Offer of Privacy Terms.

**Subprocessor:** For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Operator, who Operator uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

**Targeted Advertising**: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Operator's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

**Texas Student Privacy Alliance:** The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

## EXHIBIT "D"

### SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

**Instructions:** This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

_____ directs _____ to
　　　　　　LEA　　　　　　　　　　　　　　　　　　　　　　　OPERATOR

dispose of　data obtained by Operator pursuant to the terms of the Service Agreement between
　return　　LEA and Operator. The terms of the Disposition are set forth below:

### 1. Extent of Return or Disposition

☐　Return or Disposition is partial. The categories of data to be disposed of are set forth below or

are found in an attachment to this Directive:

```
┌─────────────────────────────────────────────────┐
│                                                 │
└─────────────────────────────────────────────────┘
```

☐　Return or Disposition is Complete. Disposition extends to all categories of data.

### 2. Nature of Return or Disposition

☐　Disposition shall be by destruction or deletion of data.

☐　Return shall be by a transfer of data. The data shall be transferred to the following
　　site as follows:

```
┌─────────────────────────────────────────────────┐
│                                                 │
└─────────────────────────────────────────────────┘
```

### 3. <u>Timing of Return or Disposition</u>

Data shall be returned or disposed of by the following date:

☐ As soon as commercially practicable

☐ By the following agreed upon date: [ ]

### 4. <u>Signatures</u>

| | |
|---|---|
| _____ | _____ |
| Authorized Representative of LEA | Date: |

### 5. <u>Verification of Disposition of Data</u>

| | |
|---|---|
| _____ | _____ |
| Authorized Representative of Operator | Date: |

**EXHIBIT " E"**

GENERAL OFFER OF PRIVACY TERMS

**Instructions:** This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

**1. Offer of Terms**
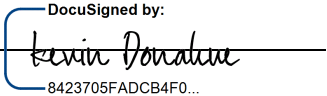Operator offers the same privacy protections found in this DPA between it and
[
and which is dated [ 10/18/23 ] to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the event of:

(1) a material change in the applicable privacy statutes;
(2) a material change in the services and products listed in the Originating Service Agreement;
(3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.

**Operator's Representative:**

BY: _____ Date: 10/18/23

Printed Name: Kevin Donahue          Title/Position: Co-Founder

**2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

**Subscribing LEA's Representative:**

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

**EXHIBIT " F"**

DATA SECURITY

1.  **Operator's Security Contact Information:**

    Norman Basch                        [Box 26]

    Named Security Contact

    privacy@getepic.com             [Box 27]

    Email of Security Contact

    973-220-7211                         [Box 28]

    Phone Number of Security Contact

2.  **List of Operator's Subprocessors:**

    https://www.getepic.com/third-party-service-providers    [Box 29]

3.

    **Additional Data Security Measures:**

                                                    [Box 30]

    See Below.

# Epic - Safety and Privacy Protection Practices
### Epic! Creations, Inc.

*Last Updated:* 2023-04-12

# Overview

Epic ("Epic!","GetEpic" "we," or "us" or "our") provides digital reading & learning products and services, for students and for schools via educators.  Epic's Privacy Policy prioritizes Child Safety and Protection, which is a reflection of our company and brand values.

This document conveys our commitment, information security programs and policies to protect sensitive data of all our customers (application administrators, district administrators, educators/teachers, and students). Our General Privacy Policy, School Privacy Policy and Terms of Use describe our data privacy practices which align to standard security practices of NIST Cybersecurity Framework and GDPR.

We are committed to comply and meet with the requirements of the following: laws(local, national, international laws), rights/acts and regulations to protect Epic School and Student privacy data - COPPA(Children's Online Privacy Protection Act), FERPA(Family Educational Rights and Privacy Act) and State Student privacy laws, including SOPIPA(Student Online Personal Information Privacy Act).

The sections below delineate our security programs, which meet the above requirements,  applicable to our products and services - offered on getepic.com (the "GetEpic Website"), including the GetEpic platform (the "GetEpic Platform"), and any associated mobile applications (the "GetEpic Apps") or products and services that Company may provide now or in the future (collectively, the "Service").

Our programs address the following areas: definitions, product security, infrastructure security, and IT security. These programs enable our organization to minimize and manage cybersecurity risk.

# Definitions

The following table covers important definitions on how we classify data:

| Term | Definitions |
|------|-------------|
| Customer(s) | Epic customers (current and future) who use our products, services. These include students, teachers/educators and application adminstrators. |
| Personal identifiable information (PII) | Any information relating to an identified, or identifiable, individual. This may include the individual's: <br>• Name (including initials) <br>• Identification number <br>• Location data <br>• Online identifier, such as a username <br>It may also include factors specific to the individual's physical, physiological, age, genetic, mental, economic, cultural or social identity. |
| PII Data Processing | Anything done to PII data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. The |

| | records can be in electronic or physical form and processing is either automated or manual. |
|---|---|
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. (GDPR definition) |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Data breach or security incident | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. |

We have already defined as part of our [Privacy Policy](#) how we collect, use and protect personal information as the *Data controller*.

We share user data including PII with a few other partners, vendors and trusted organizations ("Service Epics", "*Data processor*", "Third party sub-processors") to process the data on our behalf in accordance with our instructions, Privacy Policy and any other appropriate confidentiality, security or other requirements. These companies will only have access to the information they need to provide the Epic Services.

We also use "IT" business services or internal tools such as Gmail, Google Drive, Asana and Slack to operate our organization ("Internal Tools"). These Internal Tool services may incidentally contain personal information (e.g., email address or contact handle) and we apply the Data processor restrictions described above.

The list of Data processors and Internal Tools are covered in Appendix sections.

# Product security

The goal of Epic's product security efforts is to capture the security and privacy impact of new features and products as they are being created so that the Engineering Team continuously improves the product in a safe and secure manner.

## Product Development and Software Development Lifecycle

We employ agile development for our iterative product development and feature releases. We have implemented Product specs reviews which includes security reviews of features scoped for iterative releases. Our security reviews and assessments follow a shift-left testing methodology. Waiting to address software security vulnerabilities to be detected post feature goes live, can be costly and exposes organizations to unnecessary risk. Hence, it's important to develop securely from the start, which is known as shift left security. It includes threat modeling, manual and automated code review.

We use automation in our software development build pipeline that analyzes code for the following:

- open source dependencies containing vulnerabilities
- containers and infrastructure as code (IaC) (container images and Kubernetes configurations)
- secure management of secrets.

Our manual code review process checks against secure coding guidelines specific to our technology stack and programming languages.

We have regular external security assessments (currently yearly interval) for our customer facing products and services, which combines static and dynamic security methods, including penetration testing and evaluating application programming interfaces (APIs). These cover (but are not limited to) identify issues with requests, responses, interfaces, scripts, injections, authentication and session vulnerabilities.

Any external inquiries related to Epic app and website security should be emailed to security@getepic.com.

# Security Features

Epic shares data at its discretion, but only subject to prior consent of customers (parents, educators, districts where applicable). Third parties must receive prior authorization by the school district to get access to the district's data.

Epic (as Data processor) receives data from other Data Controllers and agrees to store, transmit, and display student data only via secure and FERPA compliant methods.

For all secure data stored at Epic, we have implemented permissions and audit controls based on role-based access.

We protect our computer systems, using the following methods:

- All sensitive data encrypted over HTTPS(HTTP over TLS, also known as HTTPS) across all connections and interfaces, as it transits over the internet. TLS configuration receives an A from Qualys SSL Labs. Refer to the Appendix for details.
- Protection against brute force by rate limiting login attempts.
- Internal tools access is centrally managed (SSO), requires authorization and audited.

We use Content Security Policy (CSP) to detect and prevent unauthorized Javascript from running in the context of our applications.

# Infrastructure security

## Third-Party Vulnerability Management

We monitor security release information for software in our stack as well as global vulnerability feeds. When a vulnerability that affects is released, we prioritize the rollout of the patch based on the severity, or impact, of the vulnerability in question. We have a dedicated DevOps and BYJU'S (parent company of Epic) central InfoSec team who monitor feeds and research on global vulnerabilities updates.

## Vulnerability Scanning

We use automated security scanning tools to notify us quickly of changes to, or activities in, our infrastructure that may result in a security issue. The results of these scans are regularly triaged by our InfoSec team.

## Change Management

We have a change management process for our infrastructure that includes source code control (on GitHub Enterprise), peer code review, logging, and alerts for unusual behavior. All production changes are deployed with an automated build system that detects reliability issues and reverts problematic deployments. Our deployments are scheduled at predefined intervals and ensure it has passed both manual and automated tests.

## Availability and Disaster Recovery

Our customer facing products are highly distributed, fault tolerant and we ensure at least 99.9% availability (details available on request based on internal monitoring methods).

We have established a set of practices and tools to defend against automated Denial of Service (DoS) attacks against our infrastructure.

Since our service is based entirely in the cloud, our disaster recovery plan is based on best practices from GCP for maintaining resiliency in the case of disaster. We take regular snapshots and backups of all critical data. We also have redundancy for critical services and data.

## Data Encryption in Storage and Transit

We encrypt all Personally Identifiable Information (PII) in transit outside of our private network and at rest in our private network. We use strong forms of cryptography such as AES256-GCM with access-controlled keys that are regularly audited and rotated. Refer details of TLS configuration in Appendix.

## Data Isolation

Epic uses logical separation to process data in a multi-tenant environment. We have separate environments for test, pre-production and production releases. The code controls are tested before promotion from each of the environments. Data processing occurs in kubernetes (containerized) with limited access to external resources. All system secrets and credentials are managed through GCP Secret Manager. All data is stored in the USA.

## Network Isolation

Epic limits external access to network services by running them inside of a Virtual Private Cloud (VPC) and blocking all unnecessary ports from external traffic. Access to our production network is limited to necessary personnel, logged, and secured using multiple factor authentication. We use a bastion SSH host to gate all system-level access to production infrastructure.

## Logging

Epic maintains a centralized log for product and infrastructure events and metrics. Tightly access-controlled and integrity protected log backups are persisted to access-controlled archival stores on Google Cloud Logging service with a max retention of 60 days. All system-level actions performed in production environments with elevated permissions (sudo) are logged.

## Threat Detection

We have monitoring, alerting, and response processes for suspicious activity occurring in our infrastructure.

## Secret Storage

No secret data (passphrases, API keys, QR Codes for 2-factor, etc) are sent using tools like Gmail, Dropbox or Slack. We use 1Password or GCP Secret Manager to manage credentials in accordance with our security requirements.

## Patching

We regularly update our operating systems images, container images, language runtimes, and language libraries to the latest known supported versions.

# IT security

The goal of our IT security practices is to make employees more productive and effective to respond to security incidents through internal tools and processes. We have also established clear channels for communications and escalation levels.

## Policies and Standards

Our information security policy is documented on our knowledge sharing portal. We have an Epic Data Classification standard that describes the different types of data that our employees work with and how that data should be handled.

## Device Policies

Our device policy describes best practices for device configuration and software usage. The System Administrators have MDM(Master Device Management) software to ensure security standards and permitted softwares are deployed/updated to all devices which have access to sensitive data.

## Account Policies

Our account policies state that all passwords should be securely stored and generated with a password manager, and mandates the use of 2FA for sensitive accounts. It also defines the OAuth authorization policies for accounts with sensitive data access (e.g. GSuite) and the techniques to avoid phishing.

Accounts are activated when an employee joins and deactivated when an employee leaves, using semi-automated processes and tracked through tickets for audit purposes.

## Security Training

We create a culture of security for all Epic employees through activities like security awareness training and awarding security-conscious behavior. All new hires are required to read our information security policy and undergo information security training, and existing employees have regular (annual) refresher training.

## Third-Party Software

We have a third-party software and data sub-processor security review process that must be completed before using new services at our organization. We limit the amount of data shared with sub-processors to only what is necessary to perform their services.
We identify all sub-processors (current list in Appendix) that will have access to user data and conduct due diligence to ensure that they have appropriate security measures in place. We also review sub-processor contracts to ensure that they contain appropriate data protection and security requirements.

## Background Checks

All Epic employees undergo criminal background checks and sign agreements barring any use of confidential information outside of the scope of their work with the company.

# Other Security Practices

## External Security Assessment

We conduct an annual external security assessment of our applications. We make the reports associated with these assessments available for our users, on request. Based on the assessment, the issues are resolved according to their severity level and overall security posture is evaluated.

## Incident Management and Response

Epic has a standardized process for responding to security incidents. When a security incident is suspected, teams are notified through our alerting channels (pager-duty notifications, emails or instant messaging) and a central communication channel is established. After each incident, we conduct a post-mortem analysis to identify root causes and track any related follow-up work.

If Epic believes that a customer's personal information has been accessed or modified by an unauthorized third party, we designate such breach as a security incident. In the event of a security incident we will take all necessary steps to notify the affected customers within two business days following the incident, and

recommend immediate corrective actions to mitigate the risks. We have established incident response procedures for security incidents that involve sub-processors, including notification requirements and escalation procedures.

*Incident Response Plan/Process:*

1. Inform incident in the pre-defined communication channels for incident response team members.
2. Conducting a preliminary investigation to determine the nature and scope of the incident (including identify/verify attacker profile, internal/external). Depending on the severity level we determine the incidence response process such as involving legal counsel, law enforcement, or regulatory bodies.
3. Containment, Eradication, and Recovery.
    1. We identify steps to contain the incident to prevent further damage or data loss.
    2. We also attempt to isolate or eradicate security vulnerabilities from affected systems or networks.
    3. We identify steps to recover system to normal operations and resolve the root-causes
    4. Within two business days following the incident, we will inform the affected customers and recommend corrective actions through our customer support channels.
4. Reporting
    1. We complete the root cause analysis and establish preventive measures.
    2. We report the incident to appropriate internal and external stakeholders, such as senior management, legal counsel, or regulatory bodies

In our communications with affected customers, we will include the following information:
- The nature of how the information was accessed (viewed, modified, etc)
- The actual information accessed
- What we've done to mitigate the access
- What corrective and preventive actions we will be taken to prevent future breaches
If you have any questions about Epic's security program, please send an email to [security@getepic.com](mailto:security@getepic.com).

# Data Processors(Sub-processor) and Internal Tools

## Data Processors
*Last Updated: 2023-04-15*

List of Subcontractors to whom Student Data may be disclosed: https://www.getepic.com/third-party-service-providers

# Security Details

## TLS configuration rating from Qualys SSL Labs
Latest refer [here](#)
Report Dated: 12 April 2023

**Qualys.** SSL Labs

Home      Projects      Qualys Free Trial      Contact

You are here: Home > Projects > SSL Server Test > getepic.com

## SSL Report: getepic.com
Assessed on:  Wed, 12 Apr 2023 10:14:29 UTC | Hide | Clear cache

Scan Another >>

| | Server | Test time | Grade |
|---|---|---|---|
| 1 | **2606:4700:0:0:0:0:6812:f75b**<br>Ready | Wed, 12 Apr 2023 10:05:29 UTC<br>Duration: 135.23 sec | A |
| 2 | **2606:4700:0:0:0:0:6812:f85b**<br>Ready | Wed, 12 Apr 2023 10:07:44 UTC<br>Duration: 134.814 sec | A |
| 3 | **104.18.247.91**<br>Ready | Wed, 12 Apr 2023 10:09:59 UTC<br>Duration: 134.981 sec | A |
| 4 | **104.18.248.91**<br>Ready | Wed, 12 Apr 2023 10:12:14 UTC<br>Duration: 135.92 sec | A |

SSL Report v2.1.10

# Security Training and Assessment Calendar

The following section highlights the security training and calendar for the current year (2023).

| Sl. No. | Description | Start Date | End Date | Status |
|---|---|---|---|---|
| 1. | Annual VAPT Assessment and Review (Products, Cloud Infrastructure) | Jun 2023 | Jul 2023 | Planned |
| 2. | Quarterly Security Awareness Training (required internal employees mandatory) | 26 May 2023 | 26 May 2023 | Planned |
| 3. | Monthly User Access Audit Reviews (critical internal tools and cloud infra) | 15 May 2023 | 30 May 2023 | Planned |

The following section highlights the security training and calendar for the last year (2022).

| Sl. No. | Description | Start Date | End Date | Status |
|---|---|---|---|---|
| 1. | Annual VAPT Assessment and Review (Products, Cloud Infrastructure) | Jun 2022 | Aug 2022 | Done |
| 2. | Monthly User Access Audit Reviews (critical internal tools and cloud infra) | 15 Mar 2023 | 30 Mar 2023 | Done |

| Sl. No. | Description | Start Date | End Date | Status |
|---|---|---|---|---|
| 3. | Monthly User Access Audit Reviews (critical internal tools and cloud infra) | 15 Apr 2023 | 30 Apr 2023 | Pending |

## Incident Management SLAs

We classify customer issues and security incidents as below. The incidence response management process and escalations are highlighted in the previous sections in this document.

| Type | Description | Examples | Response SLAs |
|---|---|---|---|
| High (Critical Issue) | Critical issues affecting a large number (greater than 20% of current user base) of users, or a significant impact on critical app functionality, breach of data and/or unauthorized access. | • Server is down<br>• Login not working<br>• High volumes of tickets<br>• PII Data breach<br>• Unauthorized access | Immediate - 2 hours |
| Medium | Issue affecting a smaller number of users or a minor impact on product functionality. | • A feature is not working<br>• Blocking a flow<br>• A feature is not working but only affecting few customers | 24 hours |
| Low | Minor issue or inquiry. | • Any minor bugs / feedbacks / feature requests / User Interface bugs | 48 hours |

**Miscellaneous**

Parent Access. Teacher amd/or Student users may invite a parent or guardian to create a profile to access the Student's Epic account directly, without referral to the EA. Once added, the parent or guardian may review the Education Records and/or Student Data associated with the student's Epic account and engage directly with the student and Teacher associated with the student's account.

Separate Account. If, and to the extent, a student's parent or guardian creates an Epic account linked to the student's Epic account, the student's information (including account name, reading history, usage information) will be transferred to and maintained in the parent or guardian account on behalf of the child upon termination of this Agreement.

Disclosure. Epic discloses Student Data to other authorized users associated with the student's use of the Epic Service (including, teachers, school administrators, classroom assistants) and, if a student's parent or guardian creates an account linked to the student's account, Student Data will be shared with the parent or guardian. In connection with the ordinary use of the Epic Service, the profile name of each student in a class may be viewable by other students in the same class, as well as classmate avatars and information related to participation in reading activities.

Deletion of Student Data.Epic shall delete Student Data at any time within sixty (60) days of receipt of request by the EA. EA is responsible for maintaining current class roster and notifying Epic to destroy Student Data which the EA no longer needed for the purposes of this DPA. If no such notification is received, Epic shall destroy Student Data after a period of at least one year of inactivity, in accordance with Epic's standard data retention policies and procedures. Epic is not capable of transferring Student Data in readable form to the EA. For clarity, Epic will not be required to delete any information which has been de-identified and/or disassociated with personal identifiers such that the remaining information cannot reasonably be used to identify a particular individual, nor will Epic be required to delete information that has been transferred to a personal account, except at the direction of the parent or guardian.

Advertising Limitations. Without limiting the other requirements of this section, Epic may use Student Data to make product recommendations to teachers, EA employees, or, to the extent a parent or guardian creates an account linked to a student account, to the parent or guardian.

List of Subcontractors to whom Student Data may be disclosed: https://www.getepic.com/third-party-service-providers

**DATA RETENTION POLICY FOR USER DATA**
**Epic! Creations, Inc.**

**Effective Date: May 30, 2023**

## 1. Policy

This Data Retention Policy for User Data ("Policy") has been adopted by Epic! Creations, Inc. ("Epic") to set principles for retaining, de-identifying, and deleting User Data collected and/or stored while providing the Epic Service. Epic reserves the right to revise or replace this Policy at any time. Epic intends for this Policy to comply with all applicable laws and regulations.

## 2. Purpose

The purpose of this Policy is to ensure that Identifiable User Data is only retained for as long as reasonably necessary to fulfil the purpose for which the information was collected, while allowing Epic to retain de-identified data to the extent permitted by all applicable federal and state laws and regulations, such as: (1) to improve educational products for adaptive learning purposes and for customized pupil learning; (2) to demonstrate the effectiveness of the operator's products in the marketing of those products; and (3) for the development and improvement of educational sites, services, or applications.

## 3. Administration

The Chief Technology Officer ("Administrator") oversees the administration and implementation of this Policy. The Administrator is authorized to: (1) propose changes to the Policy for the consideration of the Chief Executive Officer from time to time to facilitate the efficient and effective administration of the Policy and to maintain compliance with applicable laws and regulations; (2) monitor local, state, and federal laws and regulations affecting data retention of personally identifiable information; (3) periodically review the Policy; and (4) monitor compliance with this Policy. If the Administrator becomes aware that this Policy may be inconsistent with any applicable law or regulation, the Administrator shall promptly consult with legal counsel to evaluate whether changes to the Policy are warranted.

## 4. Applicability

This Policy applies to Identifiable User Data associated with Educational Accounts (those accounts created for or on behalf of an educational institution) and Family Accounts (those accounts created by a parent or guardian for home or personal use). Identifiable User Data is defined as:

- Student Personally Identifiable Information, which is defined as information that personally identifies an individual student or the student's parent or family and is collected or stored by Epic while providing the Epic Service. Student personally identifiable information includes any of the following information of a student: (a) first name, (b) last name, (c) geolocation information at the street level, (d) electronic contact information, such as a screen name or username provided by a user, or e-mail address, and (e) any information that would allow a reasonable person in the school community who does not have knowledge of the relevant circumstances to identify the student with reasonable certainty.

This Policy does not apply to De-Identified User Data, which is defined as:

- Information that cannot reasonably be used to identify a student, parent, family, or teacher with reasonable certainty by a reasonable person in the school community who does not have knowledge of the relevant circumstances.

To be comprehensive, the foregoing definitions of User Data are intentionally broad, include many categories of data that Epic does not and will not collect or store while providing the Epic Service, and may include information that may not be regulated under applicable laws.

The process(es) used to de-identify Identifiable User Data is designed so that the remaining data cannot be used to identify, infer information about, or otherwise be linked to an individual, and Epic commits that it will not attempt to re-identify such information.

The process(es) used to de-identify Identifiable User Data will be designed so that personally identifiable information is deleted or destroyed such that it cannot be recovered during the ordinary course of business.

In order to effectively administrate this Policy, the Administrator shall (a) create and maintain a schedule of the specific Identifiable User Data that is subject to this Policy and (b) document the de-identification processes used to effectuate this Policy in consultation with applicable stakeholders and legal counsel.

**5. Data Retention Schedules for Identifiable User Data**

Epic will implement a default data retention schedule for all Identifiable User Data associated with Educational Accounts as an added measure so that Identifiable User Data is not inadvertently retained when it is no longer necessary for the purpose for which it was created.

**Data Retention Schedule.** Educational Accounts (including any associated teacher or student users) will be de-identified 36 months after the subscription for such an account has expired (e.g., due to cancellation or expiration due to non-payment), and Educational Accounts will have student users de-identified after 36 consecutive months of inactivity.

**6. Transfer or Deletion Requests for Identifiable User Data**

Epic will comply with all appropriate deletion and transfer requests as set forth in this Section. At any time, an educational institution, eligible student, or a parent may request permanent deletion or transfer of applicable Student/Teacher Personally Identifiable Information in accordance with the Epic Service's Terms of Service via phone or email. Such requests shall be verified using Epic's then standard security process. If a parent or eligible student (>18 years old or emancipated) requests deletion or transfer of personally identifiable information for a user that is associated with an Educational Account, Epic shall refer the requesting individual to an authorized individual at the educational institution which owns and controls the account so that the educational institution may provide appropriate instructions to Epic.

In accordance with the Epic Service Terms of Service, Epic may retain financial-related residual data relating to subscription status, history, products purchased, payment history, payment methods, billing information (including account-holder personal information and contact information), and the like after a deletion request has been acted upon; such information is not subject to this Policy. Similarly, limited amounts of personal information may also be retained in other business records, such as technical support logs and customer service communications.

**7. Suspension in Event of Litigation or Claims**

Epic has a duty to preserve and halt the destruction of data relevant to a litigation matter once such litigation is initiated or reasonably anticipated. If the Administrator becomes aware that (a) litigation has been instituted, (b) believes that litigation may be reasonably anticipated (the "Claim"), the Administrator must promptly confer with legal counsel and, if warranted, order a complete or partial halt to data destruction under this Policy of data relevant to the Claim and communicate the order in writing to all affected employees. If any employee becomes aware that litigation has been instituted or believes that litigation is reasonably anticipated, the employee must inform the Administrator.

# EXHIBIT "G"
## Additional Terms or Modifications

LEA and Provider agree to the following additional terms and modifications:

**Parent Access.**
Student users may invite a parent or guardian to create a profile to access the Student's Epic account directly, without referral to the LEA. Once added, the parent or guardian may review the Education Records and/or Student Data associated with the student's Epic account and engage directly with the student and Teacher associated with the student's account.

**Separate Account.**
If, and to the extent, a student's parent or guardian creates an Epic account linked to the student's Epic account in accordance with subsection (2), the student's information (including account name, reading history, usage information) will be transferred to and maintained in the parent or guardian account on behalf of the child upon termination of this Agreement.

**No Disclosure, and Exhibit G(4) Limitations on Re-disclosure.**
Provider discloses Student Data to other authorized users associated with the student's use of the Provider Service (including, teachers, school administrators, classroom assistants) and, if a student's parent or guardian creates an account linked to the student's account, Student Data will be shared with the parent or guardian.  In connection with the ordinary use of the Provider Service, the profile name of each student in a class may be viewable by other students in the same class, as well as classmate avatars and information related to participation in reading activities.

**Disposition of Data, and Transfer or Deletion of Student Data.**
Provider shall delete Student Data at any time within sixty (60) days of receipt of request by the LEA. LEA is responsible for maintaining current class roster and notifying Provider to destroy Student Data which the LEA no longer needed for the purposes of this DPA.  If no such notification is received, Provider shall destroy Student Data after a period of at least one year of inactivity, in accordance with Provider's standard data retention policies and procedures.  Provider is not capable of transferring Student Data in readable form to the LEA.

For clarity, Provider will not be required to delete any information which has been de-identified and/or disassociated with personal identifiers such that the remaining information cannot reasonably be used to identify a particular individual, nor will Provider be required to delete information that has been transferred to a personal account, except at the direction of the parent or guardian.

**Advertising Limitations.** Without limiting the other requirements of this section, Provider may use Student Data to make product recommendations to teachers, LEA employees, or, to the extent a parent or guardian creates an account linked to a student account, to the parent or guardian.

**List of Subcontractors** to whom Student Data may be disclosed:
https://www.getepic.com/third-party-service-providers