

STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, NEW HAMPSHIRE, RHODE ISLAND AND VERMONT

MA-ME-NH-RI-VT-NDPA, Standard Version 1.0

Newton Public Schools

and

Epic! Creations, Inc.

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between Newton Public Schools, located at 100 Walnut Street, Newton, MA 02460 (the “**Local Education Agency**” or “**LEA**”) and Epic! Creations, Inc., located at 702 Marshall Street, Suite 280, Redwood City, CA 94063 (the “**Provider**”). **WHEREAS**, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Norman Basch Title: VP

Address: 702 Marshall Street, Suite 280, Redwood City, CA 94063

Phone: 973-220-7211

Email: norman@getepic.com

The designated representative for the LEA for this DPA is:

Steven Rattendi, Director of Information Technology & Library Services

Newton Public Schools, 100 Walnut Street, Newton, MA 02460

978-559-6000

rattendis@newton.k12.ma.us

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

NEWTON PUBLIC SCHOOLS

Steven Rattendi
Steven Rattendi (Jul 13, 2023 13:41 EDT)

By: _____

Date: 7/13/2023

Printed Name: Steven Rattendi

Title/Position: Director of IT/Library Services

Epic! Creations, Inc.

Kevin Donahue
Kevin Donahue (Jul 13, 2023 10:24 PDT)

By: _____

Date: 7/13/23

Printed Name: Kevin Donahue

Title/Position: Co-Founder

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- 2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- 3. DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- 1. Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement 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 Student Data transmitted to the Provider, 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 Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- 2. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data 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 reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's 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, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
- 4. Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services,

the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student 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 the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D".
7. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall

implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - 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, then 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; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to 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 Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) 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 Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

- 1. 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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
- 2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
- 3. Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
- 4. Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. 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.
- 5. 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.
- 6. Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
- 7. Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider

in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A" DESCRIPTION OF SERVICES

Epic School and Epic School Plus, a digital reading & learning platform.

EXHIBIT "B"
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. | X |
| | Other application technology meta data-Please specify: | |
| Application Use Statistics | Meta data on user interaction with application | X |
| Assessment | Standardized test scores | |
| | Observation data | |
| | Other assessment data-Please specify: | |
| Attendance | Student school (daily) attendance data | |
| | Student class attendance data | |
| Communications | Online communications captured (emails, blog entries) | |
| Conduct | Conduct or behavioral data | |
| Demographics | Date of Birth | |
| | Place of Birth | |
| | Gender | |
| | Ethnicity or race | |
| | Language information (native, or primary language spoken by student) | |
| | Other demographic information-Please specify: | |
| Enrollment | Student school enrollment | X |
| | 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 | |

| Category of Data | Elements | Check if Used by Your System |
|-----------------------------|--|------------------------------|
| | 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: | |
| Student Contact Information | Address | |
| | Email | |
| | Phone | |
| Student Identifiers | Local (School district) ID number | X |
| | State ID number | |
| | Provider/App assigned student ID number | |
| | Student app username | X |
| | Student app passwords | X |
| Student Name | First and/or Last | X |
| 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: | |
| Transportation | Student bus assignment | |
| | Student pick up and/or drop off location | |
| | Student bus card ID number | |
| | Other transportation data – Please specify: | |

| Category of Data | Elements | Check if Used by Your System |
|------------------|---|------------------------------|
| Other | Please list each additional data element used, stored, or collected by your application: | |
| None | No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable. | |

EXHIBIT "C" DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

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

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

| | MAINTAINING ORGANIZATION/GROUP | FRAMEWORK(S) |
|-------------------------------------|--|--|
| <input checked="" type="checkbox"/> | National Institute of Standards and Technology | NIST Cybersecurity Framework Version 1.1 |
| <input type="checkbox"/> | National Institute of Standards and Technology | NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171 |
| <input type="checkbox"/> | International Standards Organization | Information technology — Security techniques — Information security management systems (ISO 27000 series) |
| <input type="checkbox"/> | Secure Controls Framework Council, LLC | Security Controls Framework (SCF) |
| <input type="checkbox"/> | Center for Internet Security | CIS Critical Security Controls (CSC, CIS Top 20) |
| <input type="checkbox"/> | Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) | Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR) |

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks. **For clarity and without limitation, none of the employees of Provider will have direct contact with students.**
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

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

Article II(2). 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.

Article IV(4). No 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.

Article IV(6). Disposition of 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 three (3) years 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.

Article IV(7). Advertising Limitations. Without limiting the other requirements of this section, Provider may use Student Data to make content 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.

Exhibit G(13) Subcontractors

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

Exhibit J

Exhibit J contains Provider's Safety and Privacy Protection Practices

EXHIBIT "G"

Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks. **For clarity and without limitation, none of the employees of Provider will have direct contact with students.**
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

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

Article II(2). 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.

Article IV(4). No 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.

Article IV(6). Disposition of 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 three (3) years 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.

Article IV(7). Advertising Limitations. Without limiting the other requirements of this section, Provider may use Student Data to make content 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.

Exhibit G(13) Subcontractors

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

Exhibit J

Exhibit J contains Provider's Safety and Privacy Protection Practices

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks. **For clarity and without limitation, none of the employees of Provider will have direct contact with students.**
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

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

Article II(2). 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.

Article IV(4). No 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.

Article IV(6). Disposition of 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 three (3) years 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.

Article IV(7). Advertising Limitations. Without limiting the other requirements of this section, Provider may use Student Data to make content 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.

Exhibit G(13) Subcontractors

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

Exhibit J

Exhibit J contains Provider's Safety and Privacy Protection Practices

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks. **For clarity and without limitation, none of the employees of Provider will have direct contact with students.**
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

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

Article II(2). 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.

Article IV(4). No 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.

Article IV(6). Disposition of 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 three (3) years 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.

Article IV(7). Advertising Limitations. Without limiting the other requirements of this section, Provider may use Student Data to make content 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.

Exhibit G(13) Subcontractors

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

Exhibit J

Exhibit J contains Provider's Safety and Privacy Protection Practices

EXHIBIT "G"
New Hampshire

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

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

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.
Date of birth.
Personal street address.
Personal email address.
Personal telephone number
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "1"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
 - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
 - (2) Limit unsuccessful logon attempts;
 - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
 - (4) Authorize wireless access prior to allowing such connections;
 - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
 - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
 - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
 - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
 - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
 - (10) Perform maintenance on organizational systems;
 - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
 - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
 - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
 - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
 - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
 - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
 - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

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

Article II(2). 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.

Article IV(4). No 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.

Article IV(6). Disposition of 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 three (3) years 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.

Article IV(7). Advertising Limitations. Without limiting the other requirements of this section, Provider may use Student Data to make content 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.

Exhibit G(13) Subcontractors

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

Exhibit J

Exhibit J contains Provider's Safety and Privacy Protection Practices

EXHIBIT "I" – TEACHER DATA

| Category of Data | Elements | Check if used by your system |
|----------------------------------|--|------------------------------|
| Application Technology Meta Data | IP Addresses of users, Use of cookies etc. | X |
| | Other application technology meta data-Please specify: | |
| Application Use Statistics | Meta data on user interaction with application | X |
| Communications | Online communications that are captured (emails, blog entries) | |
| Demographics | Date of Birth | |
| | Place of Birth | |
| | Social Security Number | |
| | Ethnicity or race | |
| | Other demographic information-Please specify: | |
| Personal Contact Information | Personal Address | |
| | Personal Email | |
| | Personal Phone | |
| Performance evaluations | Performance Evaluation Information | |
| Schedule | Teacher scheduled courses | |
| | Teacher calendar | |
| Special Information | Medical alerts | |
| | Teacher disability information | |
| | Other indicator information-Please specify: | |
| Teacher Identifiers | Local (School district) ID number | x |
| | State ID number | |
| | Vendor/App assigned student ID number | |
| | Teacher app username | x |
| | Teacher app passwords | x |
| Teacher In App Performance | Program/application performance | |
| Teacher Survey Responses | Teacher responses to surveys or questionnaires | |
| Teacher work | Teacher generated content; writing, pictures etc. | |
| | Other teacher work data -Please specify: | |
| Education | Course grades from schooling | |
| | Other transcript data -Please specify: | |
| Other | Please list each additional data element used, stored or collected by your application | |

EXHIBIT J

Partner ("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 administrators. |
| Personal identifiable information (PII) | Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none">• Name (including initials)• Identification number• Location data• Online identifier, such as a username 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.

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

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 | 2606:4700:0:0:0:6812:f75b Ready | Wed, 12 Apr 2023 10:05:29 UTC Duration: 135.23 sec | A |
| 2 | 2606:4700:0:0:0:6812:f85b Ready | Wed, 12 Apr 2023 10:07:44 UTC Duration: 134.814 sec | A |
| 3 | 104.18.247.91 Ready | Wed, 12 Apr 2023 10:09:59 UTC Duration: 134.981 sec | A |
| 4 | 104.18.248.91 Ready | Wed, 12 Apr 2023 10:12:14 UTC 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. | <ul style="list-style-type: none"> • Server is down • Login not working • High volumes of tickets • PII Data breach • Unauthorized access | Immediate - 2 hours |
| Medium | Issue affecting a smaller number of users or a minor impact on product functionality. | <ul style="list-style-type: none"> • A feature is not working • Blocking a flow • A feature is not working but only affecting few customers | 24 hours |
| Low | Minor issue or inquiry. | <ul style="list-style-type: none"> • Any minor bugs / feedbacks / feature requests / User Interface bugs | 48 hours |

Miscellaneous

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 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 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.

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.

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.










Epic_Newton_Final

Final Audit Report

2023-07-13

| | |
|-----------------|--|
| Created: | 2023-07-13 |
| By: | Ramah Hawley (rhawley@tec-coop.org) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAABAKCHlx_xzbNRk7G8Kelah75HbeEPpcNle |

"Epic_Newton_Final" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2023-07-13 - 12:41:25 PM GMT- IP address: 108.35.203.7
-  Document emailed to Kevin Donahue (kevin@getepic.com) for signature
2023-07-13 - 12:45:37 PM GMT
-  Email viewed by Kevin Donahue (kevin@getepic.com)
2023-07-13 - 5:23:29 PM GMT- IP address: 107.116.89.58
-  Document e-signed by Kevin Donahue (kevin@getepic.com)
Signature Date: 2023-07-13 - 5:24:47 PM GMT - Time Source: server- IP address: 107.116.89.58
-  Document emailed to rattendis@newton.k12.ma.us for signature
2023-07-13 - 5:24:48 PM GMT
-  Email viewed by rattendis@newton.k12.ma.us
2023-07-13 - 5:38:20 PM GMT- IP address: 50.203.230.202
-  Signer rattendis@newton.k12.ma.us entered name at signing as Steven Rattendi
2023-07-13 - 5:41:34 PM GMT- IP address: 209.6.3.166
-  Document e-signed by Steven Rattendi (rattendis@newton.k12.ma.us)
Signature Date: 2023-07-13 - 5:41:36 PM GMT - Time Source: server- IP address: 209.6.3.166
-  Agreement completed.
2023-07-13 - 5:41:36 PM GMT