

EPIC

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Wayne Finger Lakes BOCES (EduTech)

and

Epic! Creations, Inc.

This Data Privacy Agreement ("DPA") is by and between the **WFL BOCES (EduTech)** ("EA"), an Educational Agency, and (Epic! Creations, Inc. ("Contractor")), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 2/5/24 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR

Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Contact: Rich Yeoman

Title: Manager of Data Services

Address: 131 Drumlin Court

City, State, Zip: Newark, NY 14513

Email: Rich.Yeoman@edutech.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its’ Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA’s notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor’s certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student’s Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	CONTRACTOR
BY: <i>Kelli Eckdahl</i>	BY:
Name: <i>Kelli Eckdahl</i>	Name: Stephen Jull
Title: <i>Director</i>	Title: Chief Business Officer
Date: <i>2/5/24</i>	Date: November 14, 2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children’s Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: Rich.Yeoman@edutech.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

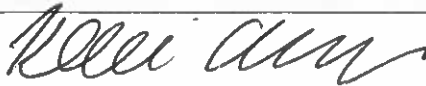
CONTRACTOR	
[Signature]	
[Printed Name]	Stephen Jull
[Title]	Chief Business Officer
Date:	November 14, 2023

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Epic! Creations, Inc.
Description of the purpose(s) for which Contractor will receive/access PII	To operate the Epic School and Epic School Plus products for schools, educators and students.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date 2.5.24 Contract End Date 2.53.25
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor may utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary,

	the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>See Exhibit C.</p>
Encryption	Data will be encrypted while in motion and at rest.


CONTRACTOR	
[Signature]	
[Printed Name]	Stephen Jull
[Title]	Chief Business Officer
Date:	November 14, 2023

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See Safety and Privacy Protection Practices below.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Safety and Privacy Protection Practices below.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See Safety and Privacy Protection Practices below.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	See Safety and Privacy Protection Practices below.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See Safety and Privacy Protection Practices below.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Safety and Privacy Protection Practices below.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Safety and Privacy Protection Practices below.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor’s Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	Yes (See Safety and Privacy Protection Practices below)
	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Yes (See Safety and Privacy Protection Practices below)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Yes (See Safety and Privacy Protection Practices below)
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Yes (See Safety and Privacy Protection Practices below)
	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Yes (See Safety and Privacy Protection Practices below)
	Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the	Yes (See Safety and Privacy Protection Practices below)

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Yes (See Safety and Privacy Protection Practices below)
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Yes (See Safety and Privacy Protection Practices below)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Yes (See Safety and Privacy Protection Practices below)
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Yes (See Safety and Privacy Protection Practices below)
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Yes (See Safety and Privacy Protection Practices below)
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Yes (See Safety and Privacy Protection Practices below)
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Yes (See Safety and Privacy Protection Practices below)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Yes (See Safety and Privacy Protection Practices below)
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Yes (See Safety and Privacy Protection Practices below)

Function	Category	Contractor Response
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Yes (See Safety and Privacy Protection Practices below)
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Yes (See Safety and Privacy Protection Practices below)
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Yes (See Safety and Privacy Protection Practices below)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Yes (See Safety and Privacy Protection Practices below)
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Yes (See Safety and Privacy Protection Practices below)
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Yes (See Safety and Privacy Protection Practices below)
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Yes (See Safety and Privacy Protection Practices below)
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Epics, owners of attacking systems, victims, other CSIRTs, and vendors).	Yes (See Safety and Privacy Protection Practices below)

Epic - Safety and Privacy Protection Practices

Epic! Creations, Inc.

Last Updated: 2023-04-12

Overview

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

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

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

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

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

Definitions

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

Term	Definitions
Customer(s)	Epic customers (current and future) who use our products, services. These include students, teachers/educators and application 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.

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

Separate Account.

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

No Disclosure, and Exhibit G(4) Limitations on Re-disclosure.

Provider discloses Student Data to other authorized users associated with the student's use of the Provider Service (including, teachers, school administrators, classroom assistants) and, if a student's parent or guardian creates an

account linked to the student's account, Student Data will be shared with the parent or guardian. In connection with the ordinary use of the Provider Service, the profile name of each student in a class may be viewable by other students in the same class, as well as classmate avatars and information related to participation in reading activities.

Disposition of Data, and Transfer or Deletion of Student Data.

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

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

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

List of Subcontractors to whom Student Data may be disclosed:

<https://www.getepic.com/third-party-service-providers>

DATA RETENTION POLICY FOR USER DATA

Epic! Creations, Inc.

Effective Date: May 30, 2023

1. Policy

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

2. Purpose

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

3. Administration

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

4. Applicability

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

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

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

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

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

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

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

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

5. Data Retention Schedules for Identifiable User Data

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

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

6. Transfer or Deletion Requests for Identifiable User Data

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

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

7. Suspension in Event of Litigation or Claims

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