wnyric
www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:
INFORMATION SECURITY PROGRAM

B.

third party wirelessly or across a public network.

Access to PII

1. *Customer -- access to PII.* Customers that provide access to PII to Newsela may contractually determine access to PII for parties beyond Newsela and its employees.

2. *Parent Inquiries*. Newsela cooperates with the customer in addressing inquiries or complaints from parents (or students 18 and over) that relate to their use or disclosures of PII.

Newsela's IT Security Program consists of technical, physical, and administrative safeguards to protect PII. Newsela's IT Security Program is designed to identify, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. Newsela's IT Security Program includes the following key general processes:

A. Information Security Risk Assessment

Newsela periodically conducts an accurate and thorough external assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Newsela; reports such risks as promptly as possible to Newsela's Security Officer or other official within Newsela designated to be responsible for data privacy and security compliance; and implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented based on the level of risks, capabilities, and operating requirements. These measures must include as appropriate and reasonable the following safeguards:

1. Administrative Safeguards

i. *Discipline*: Newsela enacts appropriate discipline with respect to employees who fail to comply with Newsela security policies and procedures.
ii. *System Monitoring*: Newsela maintains procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
iii. *Security Oversight*: Assignment of one or more appropriate senior officials within Newsela as applicable, to be responsible for developing, implementing, and monitoring of safeguards and security issues.
iv. *Appropriate Access*: Procedures to determine that the access of Newsela

employees to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Newsela employees who have access to PII.

v. *Access Termination*: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

2. Access Safeguards
    i. *Access to PII*: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
    ii. *Awareness Training*: On-going security awareness through training or other means that provide Newsela employees (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training should also address procedures for safeguarding passwords.
    iii. *Incident Response Plan*: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
    iv. *Encryption and Final Disposition of Information*: Procedures addressing encryption of all data at rest and in transit and the final disposition of PII. Procedures must include processes for the continued encryption of customer's PII through the time when its secure deletion/destruction has been requested in writing by the customer, or when the terms of the agreement between Newsela and a customer require that the PII be deleted/destroyed.
3. Technical Safeguards
    i. *Data Transmissions*: Technical safeguards to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups. Encryption is used when PII are in transit or at rest. Unencrypted PII is not transmitted over public networks to third parties.
    ii. *Data Integrity*: Procedures that protect PII maintained by Newsela from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.
    iii. iii. *Logging off Inactive Users*: Inactive electronic sessions are designed to terminate automatically after a specified period of time.

(b) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(c) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(d) Vendor _____will __x___will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(e) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(f) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the reasonable cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the

incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Signature Not Required by:
Chris Mezzatesta
34D08E5C0C40438...

Signature

Chris Mezzatesta
Printed Name

Chief Customer Officer

Title

□/2□/2020

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND NEWSELA

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Newsela which governs the availability to Participating Educational Agencies of the following Product(s):

Newsela ELA, Newsela Social Studies, Newsela Science, Newsela SEL, Newsela Essentials, Newsela Custom Collections

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontactors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontactors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontactors, assignees, or other authorized agents abide by the provisions of these agreements by: ensuring that work is contingent on proof of protection of Protected Data.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on May 6 2020 and expires on June 30 2023.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back

to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

DATA SECURITY & PRIVACY POLICY

Updated as of November 20, 2019

I. INTRODUCTION

Purpose and Approach. This sets forth the policies and procedures of Newsela, Inc.("Newsela") with respect to data security and privacy. Newsela requires that its subcontractors that receive data containing PII (defined below) maintain similar policies. This Policy describes, in general, the information that Newsela collects, how it is used and how it is protected. The principles described in this Policy apply not just to PII, but to all data provided by customers. However, the requirements and policies in this Data Privacy and Security Policy apply specifically to the use and protection of PII provided by customers.

DEFINITIONS

Capitalized terms referenced herein but not otherwise defined have the meanings as set forth below:

"Breach" means the unauthorized acquisition, access, use, or disclosure of PII which, in Newsela's judgment following due investigation, compromises the security or privacy of such information.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

"FERPA" means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S. Department of Education, and are available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

"Subcontractor" means each contractor of Newsela that may be required to maintain or handle PII in the course of providing services in support of the sublicensing of Newsela content.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA or relevant state law, including small cell-size data that are linkable to a specific student, as provided under FERPA regulations. PII includes information that alone or in combination is linked or linkable to a specific student 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.

Note: Newsela does not receive Social Security numbers.

"Security Incident" is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices or an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

Security Incidents may include a Breach or hacking of the Newsela Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Newsela's business, whether owned by Newsela or operated by its employees, agents or Subcontractors in performing work for Newsela.

"Student data" means personally identifiable information from student records of an educational agency.

II. USE OF PERSONALLY IDENTIFIABLE INFORMATION BY NEWSELA.

Student Personally Identifiable Information ("PII") may be provided by customers and used by Newsela to perform contracted services and to carry out studies designed to improve the Newsela offering and the customer experience.

Student Data is never shared without written authority from the customer unless Newsela is legally required to do so by subpoena or court order. Disclosure of PII to Newsela is authorized by the Family Educational Rights and Privacy Act ("FERPA") only for the purposes of performing institutional services for the customer as a "school official" pursuant to the conditions and restrictions set forth in § 99.31 (a) (1) (i) (B).

Newsela collects only the student data required to operate our applications. Personally identifiable student data is not shared with third parties for marketing purposes. Our student PII collection is limited to:

- First and last name
- Email (only necessary if student registers without a classroom code)
- Birth date (only necessary if student registers without a classroom code)

Additional information that may be collected includes:

- Browser user agents,
- application use statistics,
- student school enrollment,
- student grade level,
- student application username and passwords
- student in-app performance,
- student generated work,
- student response to questionnaires,
- teacher name,
- teacher email,
- teacher roster
-

Customer Ownership of the Data. All data provided to Newsela by customers, including student data, remains the property and responsibility of customers in accordance with FERPA and applicable state law. As such, each customer is responsible for ensuring its own compliance with applicable law, including FERPA.

Data Sale Newsela does not sell user data, either in anonymized or aggregate form.

Derived Models Newsela creates derivative analytical models from aggregated or anonymized data. These models constitute some of the value provided to customers via Newsela's applications. Derived models are not available for direct access by outside parties. For example, Newsela uses anonymized student quiz activity to estimate quiz question difficulty for all students on Newsela's platform.

Contractor & Non-Staff Access Contracted engineering personnel do not have access to production user data. Data is made available to contract engineers in an anonymized or contrived format.

Research Newsela does not sell data for research purposes or make data available for commercial research. User data may be used for research purposes only with explicit agreement from the data owners of the data (e.g. via specific district approval) and only for the limited duration of a defined research project (e.g. a time-bound efficacy study).

III. PRIVACY OF PERSONAL INFORMATION

A. Basic Privacy Protections

1. *Compliance with Law and Policy*. All PII uploaded to or made accessible to Newsela is handled, processed, stored, transmitted and protected in accordance with all applicable federal data privacy and security laws (including FERPA), data privacy and security laws of the state from which the data originated, and with this Policy. Newsela designs and maintains its programs, systems and infrastructure with respect to the receipt, maintenance and sharing of Protected Data to comply with all applicable data security and privacy requirements arising out of state, federal, and local law. We track those requirements internally with the assistance of outside counsel and privacy experts and maintain compliance by ensuring that privacy and security are elements of all design and redesign efforts, and through ongoing internal systems reviews and updates. Elsewhere in this document we provide detail regarding measures taken by Newsela to (i) secure Student Data and to limit access thereto (ii) implement "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff, and (iii) ensure that subcontractors, if any, receiving Student Data, if any, will abide by the legal and contractual obligations with respect to Student Data. These, taken together, amount to our "normal operating procedures." To the extent individual contracts introduce data security or privacy requirements that vary from our aforesaid normal

operating procedures, such requirements are documented and noted in our internal systems and implemented in the execution of the work under that contract.

2. *Training*. Employees of Newsela (including temporary and contract employees) are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security. Such training includes training for new employees and refresher training for current employees.

3. *Personnel Guidelines*. All Newsela employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. Newsela and its employees do not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or action by a customer that requires such access, or where they have a legitimate need for the information to maintain their data system or perform services for customers as contractually agreed upon. The following list provides a general description of internal Newsela policies:

    a. Limit internal access to PII to Newsela and its employees with proper authorization and allow use and/or disclosure internally, when necessary, solely to employees with a legitimate need for the PII to carry out the educational purposes of Newsela under its contracts with customers.

    b. Allow access to PII in Newsela's possession by parties other than the customer only where users are authorized to have access to PII by the customer.

    c. Require that materials containing PII in electronic form are stored solely within encrypted data repositories and PII are not available on unencrypted shared drives or on a local drive.

    d. When PII is no longer needed or customers request the return of PII, delete access to PII, in accordance with secure destruction procedures.

    e. Permit Newsela employees to download information onto storage only as directed by Newsela's Security Officer or his/her designee, and ensure that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).

    f. Require that any downloaded materials consisting of PII remain in the United States.

    g. Prohibit the unencrypted transmission of information from Newsela to any

third party wirelessly or across a public network.

B. Access to PII

1. *Customer -- access to PII.* Customers that provide access to PII to Newsela may contractually determine access to PII for parties beyond Newsela and its employees.
2. *Parent Inquiries.* Newsela cooperates with the customer in addressing inquiries or complaints from parents (or students 18 and over) that relate to their use or disclosures of PII.

IV. INFORMATION SECURITY PROGRAM

Newsela's IT Security Program consists of technical, physical, and administrative safeguards to protect PII. Newsela's IT Security Program is designed to identify, manage, and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. Newsela's IT Security Program includes the following key general processes:

A. Information Security Risk Assessment

Newsela periodically conducts an accurate and thorough external assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Newsela; reports such risks as promptly as possible to Newsela's Security Officer or other official within Newsela designated to be responsible for data privacy and security compliance; and implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented based on the level of risks, capabilities, and operating requirements. These measures must include as appropriate and reasonable the following safeguards:

1. Administrative Safeguards

i. *Discipline*: Newsela enacts appropriate discipline with respect to employees who fail to comply with Newsela security policies and procedures.

ii. *System Monitoring*: Newsela maintains procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.

iii. *Security Oversight*: Assignment of one or more appropriate senior officials within Newsela as applicable, to be responsible for developing, implementing, and monitoring of safeguards and security issues.

iv. *Appropriate Access*: Procedures to determine that the access of Newsela

employees to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Newsela employees who have access to PII.

v. *Access Termination*: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

2. Access Safeguards

i. *Access to PII*: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.

ii. *Awareness Training*: On-going security awareness through training or other means that provide Newsela employees (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training should also address procedures for safeguarding passwords.

iii. *Incident Response Plan*: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.

iv. *Encryption and Final Disposition of Information*: Procedures addressing encryption of all data at rest and in transit and the final disposition of PII. Procedures must include processes for the continued encryption of customer's PII through the time when its secure deletion/destruction has been requested in writing by the customer, or when the terms of the agreement between Newsela and a customer require that the PII be deleted/destroyed.

3. Technical Safeguards

i. *Data Transmissions*: Technical safeguards to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups. Encryption is used when PII are in transit or at rest. Unencrypted PII is not transmitted over public networks to third parties.

ii. *Data Integrity*: Procedures that protect PII maintained by Newsela from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.

iii. *Logging off Inactive Users*: Inactive electronic sessions are designed to terminate automatically after a specified period of time.

4. Data Storage

i. *Data Cataloging* Newsela maintains a data catalog of application data points. Data points are classified as:
   - Personal, Identifiable
   - Personal, Non-Identifiable
   - Credential
   - User Key
   - Behavioural
   - User Generated Content
   - Newsela Content

   This catalog supports the accuracy of external reporting about what we collect as required by law, contract, and our own privacy policy.

ii. *Student Data* Newsela collects only the student data required to operate our applications. Personally identifiable student data is not shared with third parties for marketing purposes.

iii. *Financial Data* Newsela does not manage financial data about users or buyers. Payments are managed by a third party. No in-application payment features exist at this time.

iv. *Privacy Policy* Newsela version-controls its privacy policy in a public repository at https://github.com/newsela/policies.

v. *Password Storage* End-user passwords are hashed using PBKDF2 with SHA256.

5. Code Access Control

i. *Code Storage* Application code is stored in private GitHub repositories. Access is managed using GitHub organizations.

ii. *Code Access* Access to repositories is granted according to least-privilege required. Newsela source code is unavailable to general staff. Repository access is approved by Engineering Operations. Newsela organization members must enable two-factor authentication in order to access repositories. Newsela repositories may be available to contracted engineers on an as-needed and temporary basis. Contractors may not receive access to repositories without cause and without being signatories to Newsela's contracting agreement. Access is revoked upon lapse of contract.

iii. *Review* Manual code review is required for production deployment. Automated style checks and automated unit and integration tests are required for production deployment. Review may be overridden only by Director-level engineering staff or on-call members of Engineering Operations.

iv. *Release Management* Releases to production Newsela applications are managed by automated processes (i.e., continuous integration systems). No manual updates to production servers or deployed code is permitted, allowing for change audits. Code deployment outside of automated pipelines is possible only for privileged members of Engineering Operations team. Manual releases are considered a reliability incident and trigger post-mortem analysis.

v. *Dependency Management* Third-party dependencies for applications must be documented in source code and version controlled. Tooling (e.g. Dependabot) automatically detects and resolves third-party dependency vulnerabilities.

6. Infrastructure

i. *Hosting* All production application infrastructure is hosted by Amazon Web Services. Data warehousing infrastructure is provided by Snowflake. Hosting providers must provide materials to Newsela documenting rigorous security and data privacy practices.

ii. *Firewalls & Network Isolation* All production and staging servers are hosted inside of an AWS Virtual Private Cloud. Newsela does not own or co-locate servers for its applications. Newsela does not maintain on-premise application infrastructure. Application production and staging networks are isolated from business networks.

iii. *Patch Management* Many of our services are hosted using Amazon Lambda, and therefore receive security updates on-demand from AWS. For our services hosted on by EC2 and ECS, application servers use Amazon Linux 2 operating system and are rotated nightly to ensure new patches are received when available. Data layer services receive weekly updates during off-peak hours (generally Saturdays at 4am).

iv. *Credentials* Newsela engineers are granted access to AWS services by the principle of least-privilege-required upon onboarding, and permissions and users are audited monthly by the site reliability team. Requests for new permissions must be submitted to the Engineering Operations team and are subject to approval by Director-level

engineering staff. Removal of credentials is part of off-boarding procedure when employment is terminated. Contracted personnel are not permitted to have credentials to production assets.

v. *Encryption* HTTPS via TLS is required to connect to all web servers from the public network. Application database is encrypted-at-rest.

B. Security Controls Implementation

Newsela has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

C. Security Monitoring

In combination with periodic security risk assessments, Newsela uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Newsela assesses on an ongoing basis whether controls are effective and performing as intended.

D. Security Process Improvement

Based on Newsela's security risk assessments and ongoing security monitoring, Newsela gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks on Newsela, and new opportunities for managing security risks and incidents. Newsela uses this information to update and improve its risk assessment strategy and control processes.

E. Incident Response and Remediation

i. *Monitoring* AWS Cloudwatch and PagerDuty monitor performance and availability. AWS GuardDuty / Macie are used for automated security alerting. These systems trigger pages to the on-call team.

ii. *On-Call Service* At least one engineer is on-call at all times who is trained to respond to operational and security issues. On-call response triggers include:

- server performance out of range
- website or service monitoring failure
- staff or external security page
- staff report of functionality failure

Newsela employees are required to report any Security Incident, or suspected Security incident, of which they become aware as promptly as possible to the

Newsela Designated Officer.

iii. *Post-Mortem Analysis* On-call responses to outages or confirmed vulnerabilities require an internally circulated post-mortem within 72 hours.

iv. *Incident Response Plan* On-call responders follow internally published Incident Response Plan, describing how incidents are identified, classified (low, high, critical), verified, and how a team is assembled to respond and communicate to outside parties. The Incident Response Plan is reviewed and rehearsed on a quarterly basis by Engineer Operations.

If Newsela determines that a Breach has occurred, Newsela will notify affected customers promptly and will cooperate with customers as needed to enable compliance with all state breach of confidentiality laws.

Note: Almost all U.S. states and other jurisdictions have laws requiring businesses to notify individuals in the event of any unauthorized acquisition of or access to files or documents containing such individuals' PII. State laws vary as to the types of PII that are covered, the methods of notification and the required contents of the notice, and whether notification is required when the PII is encrypted. Some states require notification to various third parties, such as law enforcement agencies, state attorneys general and/or credit reporting companies.

F. Organization, Responsibilities and Administration

Newsela has appointed one or more senior officials ("Designated Officer") responsible for developing, implementing and maintaining the Data Privacy and Security Program required under this Policy, under the oversight of Newsela's Chief Executive Officer.

G. Personnel Security Policy Overview

Newsela mitigates the risks posed by internal users of PII by:

1. Performing appropriate background checks and screening of Newsela employees, who are granted access to Newsela - maintained PII;

2. Obtaining agreement from Newsela internal users as to confidentiality, nondisclosure and authorized use of PII; and

3. Providing training to support awareness and policy compliance for new hires and annually for all Newsela employees.

V. ENFORCEMENT

Newsela consistently enforces this Policy with appropriate discipline for its employees. Newsela will determine whether violations of this Policy have occurred and, if so, will determine the disciplinary measures to be taken against any director, officer, employee, agent or representative who violates this Policy.

The disciplinary measures may include counseling, oral or written reprimands, warnings, probation or suspension without pay, demotions, reductions in salary, or termination of service or employment, as well as criminal referral to law enforcement, if appropriate.

Persons subject to disciplinary measures may include, in addition to the violator, others involved in the wrongdoing such as (a) persons who fail to use reasonable care to detect a violation, (b) persons who withhold material information regarding a violation, and (c) supervisors who approve or condone the violations or attempt to retaliate against employees or agents or representatives of Newsela for reporting in good faith violations or violators.

Newsela may also take appropriate actions authorized under contract or by law regarding Subcontractors that fail to comply with the terms of this Policy. It is noted that if the U.S. Department of Education finds that Newsela or a Newsela Subcontractor has violated FERPA requirements related to disclosure, Newsela or the Subcontractor, as applicable, may be debarred by the U.S. Department of Education from access to PII from the affected customer for at least 5 years.