# GARDEN CITY UNION FREE SCHOOL DISTRICT
# EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Newsela, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the GARDEN CITY UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

**"Protected Data"** includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

**-AND-**

"Personally identifiable information" from the records of the District 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of

Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

## Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

**NAME OF PROVIDER**: Newsela, Inc.

**BY:** Bryan Caplin **DATED:** 07 / 15 / 2025

**Return to:**

**Lauren Maguire**
**Director of Information Technology**
**Garden City Union Free School District**
**56 Cathedral Avenue**
**Garden City, NY 11530**
maguirel@gcufsd.net

# DATA PRIVACY AND SECURITY PLAN

**CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.**

# 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.