Cambium Assessment Privacy Policy

Objective

Cambium Assessment processes personal data on behalf of the Controller. The Controllers are State Education Boards, School Districts and Schools. As a Processor, CAI processes personal data according to the directives of the Controller.

Cambium Assessment's privacy policy provides the guiding set of privacy principles to help employees, teams, third parties and business partners to understand their privacy obligations as they develop software and testing services, develop proposals for new business, work with vendors and engage with clients and stakeholders.

The main objective of our privacy policy is to safeguard Personal Information (PI) from unauthorized access and disclosure. Cambium Assessment's Privacy Policy governs how PI shall be used, shared and retained. Privacy policy informs security systems about the security that is needed to protect sensitive information during collection, storage, use and transmission.

Our privacy policy covers the following areas:

1. Data Classification
2. Data Security
3. Data Collection principles
4. Use of cookies
5. Data Use
6. Data Retention and destruction
7. Sharing of data across Cambium Assessment groups
8. Sharing of data with third parties and vendors
9. Targeted advertising
10. Notifying changes to data security processes
11. Data breach notification
12. Data handling policies in the event of sale, merger, or bankruptcy
13. Additional Privacy Terms for Text Message Alert Service
14. Requests to access personal data (DSAR)
15. Contact Information

Data Classification

Cambium Assessment has established policies for classifying and handling personal information. Cambium Assessment's compliance with The Family Educational Rights and Privacy Act (FERPA) requires protection of students' personally identifiable information (PII) from unauthorized disclosure. By default, all user PI are considered Confidential by Cambium Assessment. This includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

Data Security

Protection of data during collection, storage and handling are described below:

All personally identifiable data are encrypted at rest, in transmission and during backup. All of our systems protect individual privacy and confidentiality in a manner consistent with the Family Educational Rights and Privacy Act (FERPA) and other federal and state laws. All secure data transmitted across the public Internet are encrypted using NIST and FIPS approved standards. All PI and FERPA protected information are encrypted at rest using FIPS compliant encryption technologies. No sensitive personal information is written to unencrypted disk. All sensitive PI are encrypted on backups.

Our systems implement configurable privacy rules that strictly limit access to data to appropriately authorized personnel. In addition to the online protection of PI, we have policies and procedures in place to prevent accidental disclosure of items. All of our personnel undergo background checks and participate in our extensive security training, which is periodically updated and revised. Every staff member's laptop has an encrypted hard drive, so files stored in temporary folders or work in progress will never be at risk if a portable computer is lost. All of our personnel are required to sign a Non-Disclosure Agreement (NDA), and NDA language is used in all contracts with third parties that involve confidential information.

Data Collection principles

All student personal and demographic information and their associations to school/district data is collected from the customer using secure methods. Our student registration system gathers data from districts, schools, or departments and stores this information in a secure roster tracking system. This data may include information about the educational networks in the State, such as which schools are in which districts, which teachers are in which schools, and which students are in which classes. This system also maintains data about the attributes of the various entities in the system, such as school addresses, student demographics, and any other information that the authorized customer provides.

Data collected during student testing is securely stored in separate systems. Other systems store only an arbitrary Cambium Assessment-assigned ID. When student data

must be matched with identifiers (e.g., when presenting an individual's results in a report), the encrypted identifiers are merged and decrypted. All PII and FERPA protected information are encrypted at rest using Federal Information Processing Standard (FIPS-140) compliant encryption technologies.

We only collect data for legitimate business use from data owners under contracts. We hold the data as trustees.

Use of cookies

CAI has a Cookie Compliance Policy that describes the use of cookies. This policy defines the types of cookies that require user consent and the associated requirements that ensure transparency, efficiency, and compliance with privacy laws.

Data Use

Personal Information collected by Cambium Assessment is strictly used for our legitimate business objectives of test delivery, test administration, students' assessment and contractual obligations.

Data Retention and destruction

Cambium Assessment holds students' data as trustees on behalf of our clients who are the school districts and states. Our data retention period will vary based on contracts with our clients and legal requirements.

Cambium Assessment has data archival and retention policies for our registration system, roster tracking system, test delivery system and analysis applications. Policies include schedules for purging data from files and databases based on what is to be purged and when. Again, this varies by contract, however, typically at the start of every school year, attributes and relationships logs and data tables from old school years are deleted. Student demographic data may be maintained across years, until the end of the contract with the customer. Analysis data is retained for 2 school years.

Sharing of data across Cambium Assessment groups

When sharing data, Cambium Assessment strictly abides by the privacy commitments made at the time of data collection in strict compliance with contractual and legal obligations.

Sharing of data with third parties and vendors

Cambium Assessment uses contracts to cover when and how personal data can be shared with external third parties and vendors. Contracts use appropriate language to ensure that third parties process the data they receive in a way that does not conflict with Cambium Assessment's privacy and data security policies. Any sharing of data with third parties is done for legitimate business reasons with the consent of the data

owner.

Targeted advertising

CAI shall not use any PI information in student records in any form of advertising.

Notifying changes to data security processes

In its role as a processor, CAI shall comply with all contractual agreements and applicable laws to protect consumers' data and continually improve our data security processes. Any material changes to our data security processes and protocols previously noted in our privacy policy shall be submitted to our controllers/consumers in advance of such changes. If you continue to use our products and services, you are agreeing to these changes.

Data breach notification

In the event of a data breach, notification to internal and external stakeholders will be conducted according to the table below:

Topic (What)
Internal and External Communications

- *Date of the breach*
- *Type of information that was breached*
- *Description of the breach*
- *Steps taken to address the breach*

Frequency (When)
Per Incident or Contract Requirement

Audience (Whom)
Impacted Stakeholders, Consumers, and Controllers

Communicator (From Who)
Top Management, Legal Counsel, Client Liaison. Contact and communication with Law Enforcement will depend on legal requirements and privacy regulations.

Communication process and contact
As appropriate. Sensitive information will be transmitted using secure channels.

Person to contact regarding the breach:
Jamal Husain
Information Systems Security
Cambium Assessment
Jamalul.husain@cambiumassessment.com

Data handling policies in the event of sale, merger, or bankruptcy

In the event of sale, merger, or bankruptcy of CAI, all our contractual obligations and commitments made to our controllers/consumers regarding data handling policies shall remain the same.

Additional Privacy Terms for Text Message Alert Service

CAI has Privacy Terms for Text Message Alert Service. Our text message alert service provides parents with notifications regarding their child's state test results.

See the Subscriber Terms and Conditions for Text Message Alert Service.

Requests to access personal data (DSAR)

A Data Subject Access Request (DSAR) is a way of giving individuals ownership of their personal information under data privacy regulations. Any individual whose personal data is collected, held, or processed by CAI can submit a DSAR request using one of the two CAI designated methods listed in Contact Information section. Requests are actively monitored on at least a daily basis.

Privacy Office: Contact Information

If you have questions about CAI's privacy policies and practices or wish to file a privacy related complaint, then you can use the following dedicated email to contact us:

Cambium Assessment Privacy Office
4200 Wilson Blvd, Suite 610,
Arlington, VA 22203
Phone: (888) 749-6178

Email: CAIPrivacyOffice@cambiumassessment.com

This privacy statement was last updated October 6, 2026.