

Privacy Policy

A comprehensive description of how Scholera collects, uses, protects, and handles personal information across our platform, products, and educational services.

Privacy is a foundational design principle at Scholera, not a compliance afterthought.

Effective September 1st, 2026

Our Commitment to Privacy

At Scholera, privacy is not a feature we added, it is a principle we built around. We are an AI-native educational technology company, and we understand that the trust of students, instructors, and institutions is the foundation on which everything else rests. The data that flows through our platform belongs to the people and institutions it describes. Our role is to steward it carefully, use it only for the purposes for which it was shared, and protect it at every layer of our system.

We are an early-stage company, and we are committed to being transparent about both what we do well and where we are still building. This policy reflects our current practices and our intended direction. Where we have identified gaps, we have named them and committed to timelines for closing them. We believe that honesty about our posture is itself a privacy value.

This policy describes how Scholera handles personal information across our websites, platform, and educational services. Institution-specific data processing agreements may include additional requirements, controls, or commitments that supplement this policy.

Scope and Applicability

This policy applies to:

- Students and instructors accessing the Scholera platform through an institutional deployment
- Institutional administrators provisioning and managing Scholera within their organization
- Visitors to Scholera's website and marketing properties
- Any individual whose personal data is processed by Scholera in connection with the delivery of our services

This policy does not apply to third-party websites, platforms, or services that Scholera links to or integrates with. Those services are governed by their own privacy policies, which we encourage users to review.

Information We Handle

The categories of information Scholera processes depend on how the platform is used and the nature of the institutional deployment. They may include:

Account and Identity Information

Information provided by institutions or users to establish and manage platform access, including name, institutional email address, role, and enrollment or course assignment data. This information is provisioned through the institution and is used solely to configure appropriate access within the platform.

Course and Learning Activity Data

Information generated through a user's interaction with the platform in the course of their educational activities. This includes queries submitted to AI tutoring features, engagement with course materials, responses to assessments, and use of project management and collaboration tools within the platform. This data is used to deliver the service and support the learning experience.

AI Interaction Data

Queries and interactions submitted to Scholera's AI features including the AI tutor and Athena, the instructor assistant. These interactions are logged by encrypted user identifier for audit and oversight purposes. Raw personally identifiable information is not passed to the underlying AI model. AI interaction data is never used to train or fine-tune any AI model.

Technical and Operational Data

Information generated automatically by the platform in the course of normal operation, including session data, platform performance metrics, error logs, and usage patterns. This information is used to operate, secure, and improve the platform and is not used to build individual profiles for any external purpose.

Communications and Support Data

Information included in support requests, feedback submissions, or direct communications with the Scholera team. This information is used to respond to requests and improve the platform experience.

How We Use Information

Scholera uses personal information only for clear educational and operational purposes directly related to the delivery of our services. Specifically, we use information to:

- Provision and manage user access within institutional deployments
- Deliver AI tutoring, instructor support, and course management features to users
- Ground AI responses in instructor-approved course materials through our retrieval augmented generation system
- Maintain the security, integrity, and performance of the platform
- Meet contractual obligations to institutional partners
- Respond to support requests and user communications
- Understand platform performance in aggregate to inform product improvement

We do not use personal information for advertising, marketing to individual users, or any purpose unrelated to the delivery of contracted educational services. We do not sell personal information. We do not build behavioral profiles for commercial purposes.

Privacy by Design

Privacy by design means that privacy protections are built into the architecture of our platform from the ground up rather than applied as a layer of controls after the fact. At Scholera, this principle shapes every major product and engineering decision.

Data Minimization

We collect and process only the information necessary to deliver the service. Every feature is evaluated at the design stage for the minimum data footprint required to function. We do not collect data speculatively or for purposes we have not defined.

Encrypted User Identifiers

User identifiers are encrypted throughout Scholera's logging and data pipeline. Interaction logs reference encrypted identifiers rather than raw personal data, ensuring that log records cannot be directly associated with an identified individual without access to decryption controls maintained separately by Scholera's engineering team.

Role-Based Access Scoping

Access to personal data within the platform is strictly scoped by user role. Students access only their own data and course context. Instructors access only data within their own course. Administrators access only data within their institutional deployment. No role has access broader than its defined function requires.

LLM Data Boundaries

Personal data is not passed to the underlying AI model in raw form. Prompts submitted to the AI inference layer are constructed at the application layer to minimize exposure of personally identifiable information. Student interaction data is never introduced into any model training pipeline. The AI model cannot access data outside the active course context defined by the instructor.

Instructor-Controlled Content

All content that the AI can access must be explicitly uploaded and activated by an instructor. The platform does not ingest external data sources, open internet content, or any materials the instructor has not reviewed and approved. This control is architectural, not procedural.

Human Oversight at Every Consequential Decision Point

No AI-generated output within Scholera triggers an automated consequential action affecting a student without instructor review. Grade decisions, academic integrity determinations, and assessment outcomes all require human approval. The AI informs; people decide.

Sharing and Third-Party Providers

Scholera does not sell personal information. We do not share personal information with third parties for advertising, marketing, or commercial purposes.

Information may be shared in the following limited circumstances:

Service Providers

Scholera works with a small number of vetted third-party providers whose services are necessary to operate the platform. These include our cloud infrastructure provider, AI inference provider (Google Gemini), database provider (Supabase), and voice generation provider (ElevenLabs). Each provider is engaged under contractual terms that include data processing obligations, confidentiality requirements, restrictions on secondary use of data, and breach notification commitments. No provider is permitted to use Scholera user data for their own commercial purposes, including model training or advertising.

Institutional Partners

Authorized personnel within a contracting institution may access data within their deployment in accordance with their role and the terms of the institutional agreement. This access is governed by the institution's own data governance policies and FERPA obligations.

Legal and Safety Requirements

Scholera may disclose information when required to do so by applicable law, court order, or governmental authority, or when necessary to protect the rights, property, or safety of Scholera, our users, or the public.

AI Model and Training Data

Scholera does not train a proprietary AI model. The platform is built on a foundational large language model provided by a vetted third-party enterprise provider. Responsibility for base model training data practices lies with the underlying model provider, whose published model governance documentation is available upon request.

Student and institutional data processed through the Scholera platform is never used to train, fine-tune, or otherwise improve any AI model, whether operated by Scholera or its providers. This commitment is reflected in our provider agreements and in the architectural design of our data pipeline.

Data Retention

Scholera retains personal information only for as long as necessary to fulfill the purpose for which it was collected, meet contractual obligations to institutional partners, or comply with applicable law.

- Course and learning activity data is retained for the duration of the contracted use period and deleted upon contract expiration unless a longer retention period is required by the institution or applicable law.
- AI interaction logs are retained for the duration of the contracted use period and are available to institutional administrators for audit and oversight purposes upon request.
- Support and communications data is retained for as long as necessary to resolve the relevant request and for a reasonable period thereafter for operational continuity.
- Technical and operational data is retained for the minimum period necessary for security, performance, and platform improvement purposes.

Institutions may request early deletion of their data at any time through Scholera's privacy contact.

Data Deletion and Individual Rights

Depending on a user's location and relationship with Scholera, they may have rights concerning their personal information including the right to access, correct, delete, or restrict its processing.

Retrieval Layer Deletion

Course materials ingested into Scholera's retrieval system can be removed by an instructor or institutional administrator at any time through the platform interface. Removal takes effect immediately, after which the AI can no longer access or reference that content.

Interaction Log Deletion

Interaction logs can be purged upon verified institutional or individual request. Scholera will confirm deletion in writing upon completion.

FERPA

Scholera operates as a school official under FERPA, processing student education records solely for the purpose of providing contracted educational services. Institutions and eligible students retain their rights under FERPA with respect to education records processed by Scholera. Requests related to FERPA rights should be directed to the contracting institution in the first instance, and to Scholera's privacy contact where Scholera's direct involvement is required.

GDPR Article 17 - Right to Erasure

For users subject to GDPR, Scholera honors verified erasure requests in accordance with Article 17. Upon receipt of a verified request, applicable personal data will be deleted from interaction logs and the retrieval layer within 30 days. Confirmation of deletion is provided in writing.

CCPA and State Privacy Laws

Users whose personal data is subject to California or other applicable state privacy laws may submit access, deletion, or opt-out requests through Scholera's privacy contact. Requests are acknowledged within five business days and handled in accordance with the requirements of the applicable law.

Base Model Layer

Because student and institutional data is never introduced into any AI model training pipeline, deletion requests at the base model layer are not applicable to Scholera's standard platform use. There is no student data embedded in model weights to be removed.

All data rights requests should be submitted to: proscio@scholera-inc.com. Requests are acknowledged within five business days and completed within 30 days unless otherwise specified in the applicable data processing agreement.

Security

Scholera applies administrative, technical, and organizational safeguards appropriate to the nature of the information we process. Our security practices include:

- Encryption of data in transit via TLS
- Encryption of data at rest via AES-256
- Encrypted user identifiers throughout the logging and data pipeline
- Role-based access controls limiting data access to defined functional roles
- Peer review of all code changes touching data handling, authentication, or AI inference
- Staging environment validation before any change is promoted to production
- Rollback capability maintained for all production deployments

We are actively building our formal security program including alignment with the NIST Cybersecurity Framework and pursuit of SOC 2 Type I certification, with milestones targeted through 2027. We are transparent that our formal security documentation is in development and welcome direct engagement from institutional security teams throughout pilot relationships.

Breach Notification

In the event of a confirmed or reasonably suspected data breach affecting institutional or student data, Scholera will notify the affected institution within 72 hours of discovery. Notification will include the nature of the breach, the categories and approximate volume of data affected, the likely consequences, and the measures taken or proposed to address it.

Following institutional notification, Scholera will work with the institution and legal counsel to assess the full scope of the breach and fulfill applicable governmental notification requirements, including notification to the New Jersey Division of State Police and other agencies as required by applicable law.

Cookies

Scholera uses cookies and similar technologies to operate and secure the platform. Cookies are used for session management and authentication, maintaining platform state within a user session, and supporting third-party authentication flows including Google OAuth. Scholera does not use cookies for advertising, cross-site behavioral tracking, or any purpose unrelated to platform operation. A full cookie inventory is available upon request from institutional partners.

Children's Privacy

Scholera's platform is designed for use in higher education contexts and is not directed at children under the age of 13. We do not knowingly collect personal information from children under 13. If we become aware that we have collected personal information from a child under 13 without appropriate consent, we will take prompt steps to delete that information.

Updates to This Policy

We will note material updates to this policy and their effective date on this page. Institutions will be notified directly of any updates that materially affect how their data is processed. Privacy questions and requests can be directed to Scholera's privacy contact at proscio@scholera-inc.com.

Contact

Scholera Inc.

Privacy Contact: Pat Roscio, COO

Email: proscio@scholera-inc.com

Location: New Jersey, United States

A dedicated Privacy Center with a structured request and concern submission form will be made available on the Scholera website by Q1 2027.