SCHOLERA

Privacy Management Program

The internal governance framework describing how Scholera inventories, classifies, processes, protects, and deletes personal data across the platform, and how we respond to individual rights requests, vendor risk, law enforcement demands, and compliance failures.

DRAFT - Effective date forthcoming

1. Purpose and Scope

1.1 Purpose

This Privacy Management Program defines how Scholera Inc. governs personal data across its platform, operations, and vendor relationships. Where the Scholera Privacy Policy describes our commitments to users and institutions, this document describes the internal processes by which those commitments are operationalized, verified, and enforced.

This program exists for three reasons. First, our institutional partners are legally accountable for the data they entrust to us, and they need to see the machinery behind our promises, not just the promises. Second, a documented process is the only reliable defense against privacy failures that arise from informal practice and undocumented assumptions. Third, we intend to grow, and the practices we formalize now will determine whether privacy scales with us or erodes as we add people and features.

1.2 Scope

This program applies to:

- All personal data processed by Scholera in any environment, including production, staging, and development
- All Scholera employees, contractors, founders, and any individual with access to Scholera systems
- All third-party vendors and subprocessors that collect, process, store, or have access to personal data on Scholera’s behalf
- All Scholera products, services, websites, and internal tools

1.3 Governance and Ownership

| Role | Owner | Responsibility |

|---|---|---|

| Privacy Program Owner | Pat Roscio, COO | Overall accountability for the privacy program, rights request handling, vendor privacy assessment, regulator and institutional communication |

| Technical Privacy Lead | Harshil Patel, CTO | Data inventory accuracy, technical control implementation, deletion execution, encryption and access control enforcement |

| Product Privacy Lead | Kevin Doshi, CEO | Privacy by design review at the feature specification stage, end user notice and consent surfaces |

| Privacy Contact of Record | proscio@scholera-inc.com | Public and institutional intake point for all privacy requests and concerns |

No individual may unilaterally approve an exception to this program. Exceptions require documented agreement from the Privacy Program Owner and the Technical Privacy Lead, and must be recorded in the exception log described in Section 14.

2. Privacy Principles

Every process in this document derives from six operating principles. When a situation arises that this program does not explicitly address, these principles govern the decision.

Collect the minimum. If a feature can work without a piece of personal data, it does not collect it. The default answer to "should we log this" is no.

Use it only for what it was given for. Data collected to deliver education services is used to deliver education services. It is not repurposed for marketing, model training, product analytics that require individual identification, or anything else, without a documented and disclosed change in purpose.

Give people control. Instructors control what the AI can see. Institutions control who has access. Individuals can ask what we hold and ask us to delete it.

Make privacy architectural, not procedural. A control enforced by code is stronger than a control enforced by a rule. Where we can make a privacy violation impossible rather than prohibited, we do.

Be honest about our posture. We are early stage. Where a control is aspirational, we say so and give a date. We do not describe planned capabilities in the present tense.

Assume the data is not ours. Student data belongs to students and to the institutions that hold their records. We are a custodian with a narrow, revocable mandate.

3. Data Inventory and Mapping

3.1 Purpose of the Inventory

Scholera cannot protect, delete, or account for data it has not catalogued. The data inventory is the authoritative record of what personal data exists in our systems, where it lives, why it is there, who can reach it, and how long it stays. Every other process in this program depends on it.

3.2 Inventory Maintenance

The data inventory is maintained by the Technical Privacy Lead and reviewed jointly with the Privacy Program Owner on the following triggers:

- Quarterly, as a standing review
- Prior to the release of any feature that introduces a new data element, storage location, or processing purpose
- Upon the addition, replacement, or removal of any vendor or subprocessor
- Following any privacy incident or data subject request that reveals an inventory gap

Any engineer who introduces a new personal data element into the platform is responsible for flagging it for inventory update as part of the pull request that introduces it. Reviewers are responsible for asking. A feature that adds a data element without an inventory entry should not pass review.

3.3 Data Flow Summary

Personal data enters Scholera through four pathways and only four:

1. Institutional provisioning. Account and enrollment data supplied by the contracting institution or synced through the LMS integration.

2. User authentication. Identity assertions from the connected identity provider at login.

3. User activity. Data generated by students and instructors as they use the platform.

4. Instructor content upload. Course materials uploaded by instructors into the retrieval layer.

Personal data leaves Scholera through three pathways and only three:

1. Display to authorized users within the scope of their role.

2. Transmission to contracted subprocessors for defined service delivery functions.

3. Export to the institution at their request, or deletion at the end of the retention period.

There is no pathway by which personal data flows to advertisers, data brokers, model training pipelines, or any party outside the contracted service relationship. This is an architectural statement, not merely a policy commitment.

3.4 Personal Data Inventory Table

The following table is the working inventory. It is intended to be edited and maintained as the platform evolves. Fields marked [VERIFY] require confirmation from the Technical Privacy Lead before this document is shared externally.

| # | Data Element | Category | Source | Purpose | Legal Basis | Storage Location | Encrypted | Access Roles | Retention | Passed to LLM | Subprocessor Exposure |

|---|---|---|---|---|---|---|---|---|---|---|---|

| 1 | Full name | Identity | Institution / IdP | Account identification, display within course | Contract / FERPA school official | Supabase | At rest | Self, Instructor (own course), Admin (own institution) | Contract term | No | Supabase |

| 2 | Institutional email address | Identity | Institution / IdP | Authentication, account recovery, service notices | Contract / FERPA school official | Supabase | At rest | Self, Admin | Contract term | No | Supabase, Google |

| 3 | Internal user ID | Identity | System generated | Primary record key | Contract | Supabase | At rest | System, Admin | Contract term | No | Supabase |

| 4 | Encrypted user identifier | Pseudonymous identifier | System generated | Audit logging, interaction attribution without PII exposure | Legitimate interest / Contract | Supabase (logs) | Yes | Engineering (with decryption control) | Contract term | No | Supabase |

| 5 | Role assignment (student / instructor / admin) | Access control | Institution / IdP | Role based access scoping | Contract | Supabase | At rest | Self, Admin | Contract term | No | Supabase |

| 6 | Course enrollment and section data | Academic record | Institution / LMS | Course provisioning, access scoping | Contract / FERPA school official | Supabase | At rest | Self, Instructor, Admin | Contract term | No | Supabase |

| 7 | AI tutor query text | Interaction data | User activity | Deliver AI tutoring response | Contract | Supabase (logs) | At rest | Engineering, Admin (on request) | Contract term | Yes | Supabase, Google Gemini |

| 8 | AI tutor response text | Interaction data | System generated | Deliver service, support audit | Contract | Supabase (logs) | At rest | Engineering, Admin (on request) | Contract term | N/A (output) | Supabase, Google Gemini |

| 9 | Athena instructor query text | Interaction data | User activity | Deliver instructor assistant response | Contract | Supabase (logs) | At rest | Engineering, Admin (on request) | Contract term | Yes | Supabase, Google Gemini |

| 10 | Course material content (instructor uploaded) | Content / possible academic record | Instructor upload | RAG grounding for AI responses | Contract | Vector store | At rest | Instructor (own course), Engineering | Until instructor deletion or contract end | Yes | Supabase, Google Gemini |

| 11 | Assessment responses and submissions [VERIFY] | Academic record | User activity | Deliver assessment features | Contract / FERPA school official | Supabase | At rest | Self, Instructor, Admin | Contract term | Conditional [VERIFY] | Supabase, Google Gemini |

| 12 | AI usage detection indicators [VERIFY] | Derived data | System generated | Surface AI usage for instructor review | Contract | Supabase | At rest | Instructor, Admin | Contract term | No | Supabase |

| 13 | Project and task data (Scholera Project) | Activity data | User activity | Deliver project management features | Contract | Supabase | At rest | Self, Team members, Instructor | Contract term | Conditional [VERIFY] | Supabase |

| 14 | Voice synthesis input text [VERIFY] | Interaction data | System generated from course content | Deliver voice features | Contract | Transient | In transit | Engineering | Not retained by Scholera [VERIFY] | No (separate service) | ElevenLabs |

| 15 | Session and authentication tokens | Technical | System generated | Maintain authenticated session | Contract / Legitimate interest | Client + Supabase | Yes | System | Session duration | No | Supabase, Google |

| 16 | IP address [VERIFY] | Technical | Automatic | Security, abuse prevention, diagnostics | Legitimate interest | Application logs | At rest | Engineering | [VERIFY] | No | Supabase / hosting provider |

| 17 | Device and browser metadata [VERIFY] | Technical | Automatic | Compatibility, diagnostics | Legitimate interest | Application logs | At rest | Engineering | [VERIFY] | No | Supabase / hosting provider |

| 18 | Error and diagnostic logs | Technical | System generated | Platform reliability | Legitimate interest | Application logs | At rest | Engineering | [VERIFY] | No | Hosting provider |

| 19 | Support request content | Communications | User submitted | Respond to support requests | Contract / Legitimate interest | Email / support system | In transit | Founding team | Contract term + reasonable period | No | Email provider |

| 20 | Institutional contact details | Business contact | Institution | Contract administration, service notices | Contract / Legitimate interest | Business systems | At rest | Founding team | Relationship duration + legal retention | No | Business tooling |

| 21 | Website analytics data [VERIFY] | Technical / marketing | Automatic | Understand site performance | Consent (where required) | [VERIFY] | [VERIFY] | Founding team | [VERIFY] | No | [VERIFY] |

Table maintenance note: Rows 11 through 21 include elements whose technical handling should be confirmed with the Technical Privacy Lead before this inventory is represented as complete to an external party. An inventory that overstates its own accuracy is worse than an inventory that flags its gaps.

3.5 Data We Deliberately Do Not Collect

Documenting what we refuse to collect is as important as documenting what we do. Scholera does not collect:

- Government identification numbers, including Social Security numbers
- Financial account or payment card data from individual users
- Biometric identifiers
- Precise geolocation data
- Health data, except where an instructor voluntarily uploads course content that happens to contain it, which is outside our control and covered by instructor content responsibilities
- Data about individuals who are not users of the platform
- Behavioral data for advertising or cross-site tracking purposes

If a future feature would require any of the above, it triggers a mandatory Data Privacy Impact Assessment under Section 8 before any development work begins.

4. Legal Basis and Purpose Limitation

4.1 Legal Basis for Processing

Scholera processes personal data under the following bases, which vary by jurisdiction and data category:

Contractual necessity. The majority of Scholera’s processing is necessary to perform the contract between Scholera and the contracting institution, and to deliver the service that users are accessing. This covers account provisioning, service delivery, AI feature operation, and platform functionality.

FERPA school official exception. In the United States, Scholera processes student education records as a school official under FERPA, performing an institutional function that the institution would otherwise perform itself, under the direct control of the institution with respect to the use and maintenance of those records. Scholera does not redisclose education records except as permitted by FERPA and the institutional agreement.

Legitimate interest. A narrow set of technical and security processing, including security logging, abuse prevention, and platform diagnostics, is conducted under a legitimate interest basis where permitted. Scholera has assessed that this processing is necessary, proportionate, and does not override the rights and freedoms of data subjects.

Consent. Where consent is the applicable basis, including for non-essential cookies and any optional feature that processes data beyond service necessity, Scholera obtains explicit, informed, and revocable consent as described in Section 9.

Legal obligation. Processing necessary to comply with applicable law, including retention obligations and lawful response to valid legal process as described in Section 6.

4.2 Purpose Limitation

Every data element in the inventory has a stated purpose. Processing that data for any purpose not stated in the inventory is prohibited without going through the purpose change process below.

4.3 Purpose Change Process

If Scholera wishes to process existing personal data for a new purpose, the following steps are mandatory and sequential:

1. Document the proposed new purpose and the specific data elements involved.

2. Assess compatibility. Is the new purpose compatible with the original purpose from the perspective of the data subject? If a reasonable student would be surprised, it is not compatible.

3. Determine legal basis. Does the existing legal basis cover the new purpose, or is a new basis required?

4. Conduct a DPIA under Section 8 if the new purpose involves sensitive data, AI processing, or a material change in data subject impact.

5. Notify institutions. Institutional partners must be informed of any material change in processing purpose affecting their data, with sufficient notice to object.

6. Update the inventory, privacy policy, and end user notice before processing begins.

7. Obtain approval from the Privacy Program Owner and Technical Privacy Lead, recorded in writing.

Processing may not begin until all seven steps are complete. There is no expedited path.

4.4 Prohibited Purposes

The following purposes are prohibited absolutely and may not be authorized through the purpose change process. Changing any of these requires a board-level decision and a public amendment to the Privacy Policy with advance notice to all institutional partners:

- Training or fine-tuning any AI model on student or institutional data
- Selling, licensing, or otherwise monetizing personal data
- Sharing personal data with advertisers or data brokers
- Building behavioral profiles of individuals for commercial purposes
- Using student data to market to students
- Any processing that discriminates against individuals or groups on a protected basis

5. Individual Rights Management

5.1 Rights Recognized

Scholera recognizes and supports the following rights, subject to applicable law and the terms of the institutional agreement:

| Right | FERPA | GDPR | CCPA / State Laws | Scholera Position |

|---|---|---|---|---|

| Access / know what is held | Yes | Art. 15 | Yes | Supported |

| Correction / rectification | Yes | Art. 16 | Yes | Supported |

| Deletion / erasure | Limited | Art. 17 | Yes | Supported at application layer |

| Restriction of processing | - | Art. 18 | - | Supported |

| Data portability | - | Art. 20 | Yes | Supported via export |

| Objection to processing | - | Art. 21 | - | Supported |

| Opt out of sale or sharing | - | - | Yes | Not applicable - Scholera does not sell or share |

| Non-discrimination for exercising rights | - | - | Yes | Committed |

5.2 The Institutional Relationship

Scholera processes most personal data on behalf of a contracting institution. This has an important consequence for rights requests: for student education records, the institution is the data controller and Scholera is the processor. Individuals exercising rights over their education records should generally direct requests to their institution, which holds the primary relationship and the legal obligation.

Scholera will not unilaterally delete, modify, or disclose institutional data in response to an individual request without coordinating with the institution, except where applicable law requires Scholera to act directly. This is a protection, not an obstacle: it prevents Scholera from becoming a mechanism by which a student's academic record can be altered outside their institution's governance.

Scholera will always acknowledge a direct individual request, explain the routing, and coordinate with the institution rather than simply refusing.

5.3 Request Intake

All privacy rights requests are received at proscio@scholera-inc.com. A dedicated Privacy Center request form will be available on the Scholera website by Q1 2027.

Requests may also arrive through an institutional administrator on behalf of an individual, or from a regulator. All are handled under the same process.

5.4 Request Handling Process

| Step | Action | Owner | Timeline |

|---|---|---|---|

| 1 | Log request in the Privacy Request Register with date, requester, nature, and applicable law | Privacy Program Owner | Same business day |

| 2 | Acknowledge receipt to the requester | Privacy Program Owner | Within 5 business days |

| 3 | Verify requester identity per Section 5.5 | Privacy Program Owner | Within 5 business days |

| 4 | Determine controller relationship and notify institution if applicable | Privacy Program Owner | Within 5 business days |

| 5 | Scope the request against the data inventory | Technical Privacy Lead | Within 10 business days |

| 6 | Execute the request across all systems and subprocessors | Technical Privacy Lead | Within 25 days of verification |

| 7 | Confirm completion to requester in writing | Privacy Program Owner | Within 30 days of verification |

| 8 | Record outcome and close in the Register | Privacy Program Owner | On completion |

Standard completion window: 30 days from verified request. Where applicable law permits an extension for complex requests, Scholera will notify the requester of the extension and the reason before the original deadline expires. Extensions are not granted for internal convenience.

5.5 Identity Verification

Scholera verifies requester identity before acting on any request, because acting on an unverified request is itself a privacy breach. Verification is proportionate to the sensitivity of the request:

- Access requests: verification through the requester's authenticated institutional account, or through institutional administrator confirmation.
- Deletion requests: authenticated account verification plus institutional confirmation where the data is an education record.
- Requests from third parties on behalf of an individual: documented authorization from the individual plus verification of both parties.

Where identity cannot be verified to a reasonable standard, Scholera will decline the request, explain why, and describe what verification would be sufficient. Scholera does not collect additional personal data for verification purposes beyond what is necessary, and any data collected solely for verification is deleted once verification is complete.

5.6 Refusals

Scholera may decline a request where:

- Identity cannot be verified
- The request would require deleting or altering an education record without institutional authorization
- Applicable law requires retention of the data
- The request is manifestly unfounded or excessive, particularly where repetitive

Every refusal is documented in the Register with the reason, communicated to the requester in writing with an explanation, and includes information about how to escalate, including to the relevant supervisory authority where applicable.

5.7 Execution Across Subprocessors

A deletion request is not complete when Scholera's own systems are clear. The Technical Privacy Lead is responsible for confirming that the request has propagated to all subprocessors identified in the inventory for the affected data elements. Where a subprocessor's deletion timeline extends beyond Scholera's 30-day commitment, this is documented in the Register and communicated to the requester with the subprocessor's expected completion date.

6. Law Enforcement and Legal Process Engagement

6.1 Position

Scholera does not voluntarily disclose personal data to law enforcement or government agencies. We require valid legal process before disclosing any user or institutional data, and we resist requests that are overbroad, improperly issued, or legally deficient.

This position exists because our users are students and educators, our institutional partners are legally accountable for the records we hold, and the trust that makes an educational platform work is destroyed the moment data flows to authorities without process.

6.2 Standard Required

Scholera will not disclose personal data to law enforcement or government agencies in the absence of one of the following:

- A subpoena validly issued and served under applicable law, for records within the scope the subpoena may reach
- A court order issued by a court of competent jurisdiction
- A search warrant issued upon probable cause by a court of competent jurisdiction
- Other compulsory legal process valid and enforceable under applicable law

Informal requests, including requests by letter, email, phone call, or in-person visit without accompanying legal process, will be declined and routed through the process below. A badge is not legal process. Urgency asserted by the requester is not legal process.

6.3 Content vs. Records

Scholera applies a heightened standard to the contents of user communications and AI interactions. Consistent with the principles underlying the Stored Communications Act and applicable case law, Scholera's position is that disclosure of the content of user interactions, including AI tutor queries and uploaded course materials, requires a search warrant rather than a subpoena. Scholera will assert this position in response to any subpoena seeking content and will require the requesting authority to obtain a warrant.

6.4 Handling Procedure

| Step | Action | Owner | Timeline |

|---|---|---|---|

| 1 | Any employee receiving a law enforcement request immediately forwards it to the Privacy Program Owner and does not respond substantively, confirm or deny the existence of records, or take any action | All employees | Immediately |

| 2 | Log the request in the Legal Process Register with date, requesting agency, contact, form of process, and scope | Privacy Program Owner | Same day |

| 3 | Engage legal counsel before any response is issued | Privacy Program Owner | Within 1 business day |

| 4 | Assess validity: proper issuing authority, jurisdiction, scope, service, and whether the standard in 6.2 and 6.3 is met | Legal counsel + Privacy Program Owner | Within 5 business days |

| 5 | Notify the affected institution and, where permitted, the affected individual, per Section 6.5 | Privacy Program Owner | Before disclosure |

| 6 | If deficient, object, move to quash, or require the authority to obtain proper process | Legal counsel | Within the response window |

| 7 | If valid, scope the production to the narrowest set of records the process actually compels | Technical Privacy Lead + counsel | As required |

| 8 | Produce records, log exactly what was produced, and retain the record permanently | Privacy Program Owner | As required |

6.5 User and Institutional Notification

Scholera's default is to notify. Where Scholera receives legal process for data belonging to a user or institution, Scholera will notify the affected institution, and where appropriate the affected individual, before producing any records, so that they have an opportunity to object or seek protective relief.

Scholera will delay or withhold notification only where prohibited by law, such as under a valid non-disclosure order or gag provision. In those cases, Scholera will:

- Assess whether the non-disclosure provision is itself valid and limited in duration
- Challenge indefinite or improperly issued gag orders where legally viable
- Notify the affected parties as soon as the prohibition lapses

6.6 Emergency Requests

Scholera recognizes that applicable law permits voluntary disclosure in narrow emergency circumstances involving an imminent risk of death or serious physical injury. Scholera will consider such requests only where:

- The request is in writing and describes the specific emergency
- The nature of the emergency is credible on its face
- Legal counsel is engaged before disclosure wherever the timeline permits
- Disclosure is limited to the minimum data necessary to address the emergency

Every emergency disclosure is logged, reviewed after the fact, and reported to the affected institution as soon as permissible. Emergency disclosure is an exception exercised rarely and documented completely, not a routine channel.

6.7 Transparency Reporting

Scholera commits to publishing a periodic transparency report summarizing the number and type of legal process requests received, the number complied with in full or in part, and the number challenged or refused. First publication targeted for Q4 2027. Where the volume of requests is low enough that reporting could identify individual cases, Scholera will report in aggregate bands rather than exact figures.

6.8 Institutional Requests

Requests from a contracting institution for data within their own deployment are not law enforcement requests and are handled through the standard support and data request process. Where an institution requests data in connection with a disciplinary, legal, or investigative matter, Scholera will fulfill the request within the scope of the institutional agreement, since the institution is the controller of that data.

7. Vendor and Third-Party Management

7.1 Principle

Every vendor with access to personal data is an extension of Scholera's privacy posture. A vendor failure is a Scholera failure from the perspective of our institutional partners. We therefore keep the vendor surface deliberately small and assess each one before engagement.

7.2 Current Subprocessors

| Vendor | Function | Personal Data Accessed | DPA in Place | Training Use Prohibited | Review Status |

|---|---|---|---|---|---|

| Supabase | Database, auth, storage | All stored personal data | [VERIFY] | N/A | Active |

| Google (Gemini) | LLM inference | Query text, course content passed at inference | [VERIFY] | [VERIFY - confirm contractual] | Active |

| Google (OAuth) | Identity provider | Email, identity assertions | [VERIFY] | N/A | Active |

| ElevenLabs | Voice synthesis | Text passed for synthesis | [VERIFY] | [VERIFY] | Active |

| Hosting provider [VERIFY] | Infrastructure | All data at rest and in transit | [VERIFY] | N/A | Active |

[VERIFY] entries must be confirmed by the Technical Privacy Lead and, where a formal DPA is not in place, remediated before this table is shared with an institutional partner. A subprocessor operating under standard consumer or free-tier terms rather than an enterprise DPA is a material gap and should be treated as a remediation priority.

7.3 Vendor Onboarding Assessment

No vendor receives access to personal data until the following assessment is completed and documented:

1. Necessity. Can the function be delivered without giving this vendor access to personal data? If yes, do that instead.

2. Data scope. Precisely which data elements will the vendor access? Document them in the inventory before engagement.

3. Contractual review. Does the vendor offer a DPA or equivalent? Does it include purpose limitation, confidentiality, security standards, breach notification with a defined timeline, subprocessor disclosure, and deletion on termination?

4. Training and secondary use. Does the agreement prohibit the vendor from using Scholera data for their own model training, product improvement requiring identification, or advertising?

5. Security posture. Does the vendor hold recognized certifications or publish security documentation? What is their breach history?

6. Sub-subprocessors. Who does the vendor use, and does the agreement require notice of changes?

7. Jurisdiction. Where is data stored and processed? Does this create cross-border transfer obligations?

8. Exit. How is data deleted on termination, and on what timeline?

Assessment outcomes are recorded in the Vendor Register and reviewed by the Privacy Program Owner before engagement.

7.4 Ongoing Vendor Review

Vendors are reviewed annually, and immediately upon:

- Notification of a change to the vendor’s terms, security posture, or subprocessors
- A publicly reported breach or security incident affecting the vendor
- A material change in the data Scholera sends to the vendor
- Contract renewal

Annual review confirms that contractual terms remain adequate, that the data elements sent still match the inventory, and that the vendor’s security and compliance documentation is current.

7.5 Vendor Offboarding

On termination of a vendor relationship, the Technical Privacy Lead confirms: access credentials revoked, data deleted or returned per the agreement, deletion confirmed in writing by the vendor, inventory updated, and institutional partners notified if the change affects the subprocessor list disclosed to them.

7.6 Subprocessor Change Notification

Scholera will notify institutional partners in advance of adding or replacing any subprocessor with access to their data, with sufficient notice to permit objection. Institutions that object to a new subprocessor may escalate under the terms of their agreement.

8. Data Privacy Impact Assessment (DPIA)

8.1 When a DPIA Is Required

A DPIA is mandatory before development begins on any of the following:

- Any feature that introduces a new category of personal data
- Any feature involving AI processing of personal data in a new way, including new model integrations
- Any processing involving sensitive or special category data
- Any feature involving automated decision-making that materially affects an individual
- Any new subprocessor with access to personal data
- Any change in data retention that extends a retention period
- Any processing of data belonging to individuals in a new regulatory jurisdiction
- Any proposed purpose change under Section 4.3 that fails the compatibility test

When in doubt, run the assessment. A DPIA that concludes "low risk, proceed" costs a few hours. A privacy failure discovered post-launch costs an institutional relationship.

8.2 DPIA Template

Each DPIA documents the following:

Section A - Description

- Feature or change under assessment
- Data elements involved and their source
- Processing purpose and legal basis
- Volume and categories of data subjects affected
- Systems and subprocessors involved
- Retention period

Section B - Necessity and Proportionality

- Why is this processing necessary to achieve the purpose?
- What less privacy-invasive alternatives were considered, and why were they rejected?
- Is the data collected the minimum required?
- Is the retention period the shortest workable?

Section C - Risk Identification

- What could go wrong for the data subject? Consider: unauthorized access, unintended inference, misuse by an authorized user, inaccurate data leading to a wrong outcome, chilling effect on legitimate use, discriminatory impact.
- For AI features specifically: could the model surface data to a user who should not see it? Could an output be inaccurate in a way that harms a student? Could the feature be used to surveil rather than support?
- What is the likelihood and severity of each risk?

Section D - Mitigations

- What architectural controls reduce each identified risk?
- What procedural controls apply?
- What human oversight exists before a consequential outcome?
- What residual risk remains after mitigation?

Section E - Consultation

- Were institutional partners consulted where the change affects their data?
- Was legal counsel engaged where the risk profile warrants it?

Section F - Outcome

- Proceed / Proceed with conditions / Do not proceed
- Conditions and their owners
- Approval signatures: Privacy Program Owner and Technical Privacy Lead
- Scheduled review date

8.3 DPIA Governance

Completed DPIAs are retained permanently in the DPIA Register. A DPIA reaching a "proceed with conditions" outcome may not ship until every condition is verified complete. DPIAs are revisited when the underlying feature changes materially.

8.4 AI-Specific Assessment Considerations

Because Scholera’s core product is AI-driven, every AI feature DPIA additionally addresses:

- Grounding scope. What content can the model access, and who authorized it?
- Boundary integrity. Can any input cause the model to access data outside the intended scope?
- Output impact. Can the output affect a student’s grade, standing, or record, and if so what human review precedes that effect?

- Inference risk. Could the feature allow an authorized user to infer information about a data subject that they are not entitled to?
- Log exposure. What is written to logs, and is it pseudonymized?
- Prompt construction. What personal data, if any, enters the prompt, and can it be reduced further?

9. End User Privacy Notice, Consent, and Choices

9.1 Notice Principle

People cannot exercise choice over processing they do not know about. Scholera's notice obligation is not satisfied by a policy page that no one reads. Notice must be delivered at the moment it is relevant, in language the reader can act on.

9.2 Layered Notice Approach

Scholera delivers privacy notice in three layers:

Layer 1 - In-context notice. Short, plain-language notice presented at the moment of collection or first use of a feature. Example: when a student first opens the AI tutor, a brief notice explains that queries are logged for audit purposes, that responses draw only on instructor-approved course materials, and that queries are not used to train AI models.

Layer 2 - Privacy summary. A concise, readable summary of what Scholera collects, why, and what choices exist, accessible at all times from within the platform.

Layer 3 - Full Privacy Policy. The complete policy document, publicly available and linked from every layer above.

9.3 Consent Standards

Where consent is the legal basis for processing, Scholera requires that consent be:

- Freely given. Access to core educational functionality is never conditioned on consent to non-essential processing.
- Specific. Consent is requested for a named purpose, not bundled into a general acceptance.
- Informed. The request states what data, what purpose, what retention, and who receives it.
- Unambiguous. Consent requires an affirmative action. Pre-ticked boxes, continued use, and silence are not consent.

- Revocable. Withdrawing consent is as easy as giving it, and the interface makes the withdrawal path visible rather than buried.

9.4 Handling Improper Consent

Consent obtained improperly is not consent, and processing conducted on its basis is unlawful processing. Scholera treats improper consent as a compliance incident under Section 13.

Implicit consent problems arise where Scholera has treated continued use, silence, or a pre-selected default as agreement. Where this is identified:

1. Immediately suspend the processing that relied on the improper consent.

2. Assess whether an alternative lawful basis genuinely covers the processing. If yes, document it and notify affected users of the correction. If no, proceed to step 3.

3. Delete or fully anonymize data collected under the improper consent, unless the user affirmatively re-consents.

4. Re-request consent through a compliant mechanism, with no dark patterns and no penalty for declining.

5. Notify affected institutions of the issue, the scope, and the remediation.

6. Log the incident, conduct a root cause review, and correct the design that permitted it.

Explicit consent problems arise where consent was collected through an affirmative action but the request was misleading, bundled, insufficiently specific, or where withdrawal was made impractical. The same six-step remediation applies. The additional obligation is to fix the consent interface itself, since an unclear consent request will keep producing invalid consent for every user who encounters it.

Consent from the wrong party arises where an individual consents to processing they lack authority over, such as a student purporting to consent to processing of another student's data, or an instructor uploading third-party content without rights. Where identified, processing is suspended, the data is removed, and the responsible party is notified of the correct process.

9.5 User Choices Available

| Choice | Availability | Mechanism |

|---|---|---|

| Decline non-essential cookies | All users | Cookie consent interface [in development] |

| Access data held about them | All users | Request to privacy contact |

| Request correction of inaccurate data | All users | Request to privacy contact or institution |

| Request deletion | Subject to institutional and legal constraints | Request to privacy contact |

| Withdraw consent for optional features | Where consent-based processing exists | In-platform setting [in development] |

| Object to legitimate-interest processing | Where applicable | Request to privacy contact |

| Export their data | All users | Request to privacy contact |

Items marked [in development] are acknowledged gaps with a target of Q1 2027. Until the in-platform mechanisms exist, the privacy contact route is available and is honored on the same timelines.

9.6 No Dark Patterns

Scholera commits that consent and privacy interfaces will not use design techniques that steer users toward less privacy-protective choices. Specifically: decline options are as prominent as accept options, privacy-protective settings are not visually de-emphasized, withdrawal is not made more effortful than consent, and no interface implies that declining will degrade core functionality when it will not.

10. Data Request Process (Institutional and Internal)

10.1 Scope

This section covers requests for data that are not individual rights requests under Section 5 and not legal process under Section 6. It principally covers institutional requests for audit logs, usage reporting, data exports, and investigative support, and internal requests by Scholera personnel for access to production data.

10.2 Institutional Data Requests

| Request Type | Requester | Verification | Turnaround | Owner |

|---|---|---|---|---|

| AI interaction audit log export | Institutional admin | Confirm admin role and institutional scope | 10 business days | Technical Privacy Lead |

| Usage and consumption reporting | Institutional admin | Confirm admin role | 5 business days | Technical Privacy Lead |

| Full data export (contract end or migration) | Institutional admin or contract signatory | Confirm authority against contract record | 20 business days | Technical Privacy Lead |

| Investigative support for a specific matter | Institutional admin | Confirm admin role and documented purpose | Case by case, acknowledged in 5 business days | Privacy Program Owner |

| Data deletion (institutional scope) | Contract signatory | Confirm authority against contract record; written confirmation of intent | 30 days | Technical Privacy Lead |

Every institutional request is logged in the Data Request Register with requester, scope, purpose, authorization verification, fulfillment date, and exactly what was produced.

Scholera scopes every production to the narrowest data set that satisfies the stated purpose. A request for "all student data" in service of investigating one course incident is scoped to that course, and the requester is told why.

10.3 Internal Access to Production Data

Scholera personnel access production personal data only where necessary to perform a defined function. Access is governed by:

- Least privilege. Access is scoped to role and revoked when the role changes.
- Documented justification. Access to production personal data for debugging, support, or investigation is documented with the reason and the scope.
- Preference for non-production data. Development and testing use synthetic or anonymized data. Production data is not copied into development environments.
- No casual browsing. Curiosity is not a justification. Accessing a user’s data without a work-related reason is a disciplinary matter under Section 13.

10.4 Access Review

The Technical Privacy Lead reviews the full list of individuals with production data access quarterly, confirms each is still appropriate, and revokes any access that is no longer necessary. The review is recorded.

11. Data Accuracy and Integrity

11.1 Why Accuracy Is a Privacy Issue

Inaccurate personal data in an educational system produces real harm: a misattributed AI interaction, a misassigned enrollment, or an erroneous integrity flag can affect a student's standing. Accuracy is therefore not a data quality concern separate from privacy - it is a core privacy obligation.

11.2 Sources of Truth

Scholera does not originate most identity and enrollment data. The contracting institution and its systems of record are authoritative for:

- Student and instructor identity
- Enrollment and course assignment
- Role and entitlement
- Institutional email address

Scholera's obligation is to reflect that source accurately, not to independently determine it. Where Scholera's records diverge from the institutional source, the institutional source governs and Scholera corrects.

11.3 Accuracy Controls

At provisioning. Identity and enrollment data is ingested from the institutional identity provider and LMS rather than manually entered, eliminating transcription error as a failure mode.

At authentication. Identity is asserted by the institutional identity provider at each login, so a stale or incorrect local record cannot grant access that the institution has revoked.

At attribution. Interaction data is bound to an encrypted user identifier derived from the authenticated session, ensuring that activity is attributed to the account that generated it rather than inferred.

On change. Where the institutional source updates a record, Scholera reflects the change. The Technical Privacy Lead is responsible for confirming that sync behavior is correct [VERIFY sync mechanism and cadence].

On derived data. Data Scholera generates rather than receives, including AI usage indicators, is treated as an indicator requiring human interpretation, never as an established fact. This is why no such indicator triggers an automated consequence. The instructor's judgment is the accuracy control.

11.4 Correction Process

| Step | Action | Owner | Timeline |

|---|---|---|---|

| 1 | Receive correction request from user, instructor, admin, or internal detection | Privacy Program Owner | - |

| 2 | Determine whether the data originates from the institution or from Scholera | Technical Privacy Lead | 5 business days |

| 3 | If institutional origin, route to the institution and confirm correction at source | Privacy Program Owner | 5 business days |

| 4 | If Scholera origin, verify the correct value and update | Technical Privacy Lead | 15 business days |

| 5 | Assess downstream impact: was the inaccurate data used in any consequential output or shared with any subprocessor? | Technical Privacy Lead | Concurrent |

| 6 | Notify any party who received the inaccurate data | Privacy Program Owner | On completion |

| 7 | Confirm correction to requester and log | Privacy Program Owner | Within 30 days |

11.5 Proactive Accuracy Review

Where an inaccuracy is identified, the Technical Privacy Lead assesses whether it is isolated or systemic. A systemic inaccuracy, such as a sync failure affecting a class of records, triggers a broader remediation and notification to affected institutions, and is treated as a compliance incident under Section 13.

12. Retention and Deletion

12.1 Retention Principle

Data that no longer serves the purpose for which it was collected is a liability, not an asset. Scholera retains personal data for the shortest period consistent with service delivery, contractual obligation, and legal requirement.

12.2 Retention Schedule

| Data Category | Retention Period | Trigger for Deletion |

|---|---|---|

| Account and identity data | Contract term | Contract termination or institutional deprovisioning |

| Enrollment and course data | Contract term | Contract termination |

| AI interaction logs | Contract term | Contract termination or verified deletion request |

| Instructor-uploaded course materials | Until instructor deletion or contract term end | Instructor action or contract termination |

| Assessment and submission data [VERIFY] | Contract term, or per institutional requirement | Contract termination or institutional instruction |

| Session tokens | Session duration | Session end or timeout |

| Technical and diagnostic logs [VERIFY] | [VERIFY - recommend 90 days] | Automatic expiry |

| Support communications | Contract term plus reasonable operational period | Periodic review |

| Institutional business contacts | Relationship duration plus applicable legal retention | Relationship end |

12.3 Deletion on Contract Termination

Within 30 days of contract termination, unless the institution instructs otherwise in writing, Scholera will delete all institutional personal data from production systems and confirm deletion in writing. Where the institution requests a data export prior to deletion, the export is delivered before the deletion clock begins.

Backup retention [VERIFY backup architecture and retention window] may extend the practical deletion horizon. Where this is the case, Scholera will state the backup expiry period explicitly rather than describing deletion as immediate. A deletion commitment that ignores backups is a commitment Scholera cannot honor.

12.4 Deletion Verification

Deletion is not complete until the Technical Privacy Lead confirms removal from: production database, vector store, application and interaction logs, any caching layer, backups (or documents the backup expiry date), and all subprocessors holding the data. Verification is recorded against the originating request.

13. Non-Compliance: Identification, Response, and Remediation

13.1 Definition

A privacy non-compliance event is any deviation from this program, the Privacy Policy, an institutional agreement, or applicable privacy law. It includes but is not limited to: unauthorized access to personal data, processing without a lawful basis, processing beyond a stated purpose, failure to honor a rights request within the required timeline, disclosure without proper authorization or legal process, retention beyond the schedule, a vendor operating outside its contractual terms, improper consent as described in Section 9.4, and failure to complete a required DPIA before shipping.

Not every non-compliance event is a data breach. Every one is treated seriously.

13.2 Reporting Obligation

Every Scholera employee, contractor, and founder has an affirmative obligation to report a suspected privacy non-compliance event to the Privacy Program Owner immediately upon becoming aware of it, and no later than 24 hours.

This obligation applies regardless of who caused the issue, including where the reporter caused it themselves, and including where the reporter believes the issue may be minor or already resolved.

13.3 Non-Retaliation

Scholera will not retaliate against any individual who reports a suspected privacy issue in good faith. Good-faith reporting of a problem the reporter caused is treated as mitigating, not aggravating. An engineer who reports their own mistake within an hour has protected the company; the same mistake concealed and discovered later has harmed it. The disciplinary framework in Section 13.7 reflects this explicitly.

An individual who believes they cannot report through the standard channel may report directly to any founder.

13.4 Response Process

| Phase | Action | Owner | Timeline |

|---|---|---|---|

| Detect | Log the event in the Non-Compliance Register with time of detection, reporter, and initial description | Privacy Program Owner | Within 24 hours of report |

| Contain | Stop the non-compliant processing. Revoke improper access. Suspend the affected feature if necessary. Containment precedes investigation. | Technical Privacy Lead | Immediately |

| Assess | Determine scope: what data, how many subjects, which jurisdictions, what duration, whether data left Scholera's control | Technical Privacy Lead + Privacy Program Owner | Within 72 hours |

| Classify | Assign severity per 13.5 and determine notification obligations | Privacy Program Owner + counsel | Within 72 hours |

| Notify | Execute notification obligations per 13.6 | Privacy Program Owner | Per 13.6 timelines |

| Remediate | Correct the underlying condition, not only the symptom | Technical Privacy Lead | Per remediation plan |

| Review | Root cause analysis and control improvement | Privacy Program Owner | Within 30 days of closure |

| Close | Record outcome, lessons, and control changes in the Register | Privacy Program Owner | On completion |

13.5 Severity Classification

| Severity | Definition | Examples | Response |

|---|---|---|---|

| Critical | Personal data confirmed accessed by or disclosed to an unauthorized party, or systemic unlawful processing affecting many subjects | Database exposure, disclosure without legal process, data sent to an uncontracted third party | Immediate containment, founder notification within 1 hour, counsel engaged same day, institutional notification within 72 hours per breach commitment |

| High | Significant control failure with potential but unconfirmed exposure, or unlawful processing of a limited population | Misconfigured access control, processing without valid consent, vendor operating outside DPA terms | Containment within 24 hours, assessment within 72 hours, institutional notification where their data is implicated |

| Medium | Process failure without exposure | Rights request missed deadline, DPIA not completed before ship, retention period exceeded | Remediation within 15 business days, logged and reviewed |

| Low | Documentation or administrative deviation | Inventory entry out of date, access review conducted late | Corrected within 30 days, tracked for pattern analysis |

Severity is assigned conservatively. Where classification is uncertain, the higher severity applies until assessment establishes otherwise.

13.6 Notification Obligations

Institutional notification. Where a non-compliance event affects an institution's data, Scholera notifies the institution within 72 hours of discovery, consistent with the commitment in the Privacy Policy. Notification includes the nature of the event, data categories and approximate volume affected, likely consequences, and measures taken or proposed. Scholera notifies even where the assessment is incomplete, providing an initial notification and follow-up detail rather than delaying notification to produce a complete picture.

Regulatory notification. Where applicable law requires notification to a supervisory authority, Scholera notifies within the statutory window, engaging counsel to determine applicability. This includes GDPR Article 33 where relevant, the New Jersey breach notification statute, and other applicable state requirements.

Individual notification. Where required by law or where the institution requests Scholera's support in notifying individuals, Scholera provides all information necessary. Because Scholera is typically the processor and the institution the controller for education records, individual notification is generally coordinated through and issued by the institution.

Credit bureau notification. Where a New Jersey breach affects more than 1,000 residents, notification to major credit reporting agencies is made as required by statute.

13.7 Accountability

Non-compliance arising from an individual's action is addressed proportionately to intent and impact:

- Good-faith error, promptly reported: treated as a process failure. Focus on control improvement. No disciplinary consequence.
- Negligence: retraining and closer review of the individual's work in the affected area.
- Concealment of a known issue: serious disciplinary action, up to termination. Concealment converts a manageable incident into an unmanageable one and is treated accordingly.
- Deliberate misuse of personal data: immediate access revocation and termination, with referral to authorities where the conduct is unlawful.

The distinction between error and concealment is the central one. Scholera would rather absorb ten reported mistakes than one hidden mistake.

13.8 Systemic Review

The Privacy Program Owner reviews the Non-Compliance Register quarterly to identify patterns. Three Low or Medium events sharing a root cause are treated as a single High-severity systemic finding requiring structural remediation, not three separate minor corrections.

13.9 Institutional Cooperation

Scholera cooperates fully with institutional partners investigating a privacy event affecting their data, including providing logs, timelines, technical detail, and access to the responsible personnel. Scholera does not restrict an institution’s ability to conduct its own review or fulfill its own regulatory obligations.

14. Program Governance and Change Management

14.1 Privacy Policy and Program Change Management

Changes to the Privacy Policy and to this Program follow a controlled process, because a privacy commitment that can be quietly revised is not a commitment.

| Step | Action | Owner |

|---|---|---|

| 1 | Draft the proposed change with a written rationale | Proposer |

| 2 | Classify the change as material or non-material per 14.2 | Privacy Program Owner |

| 3 | Assess impact on existing processing, institutional agreements, and disclosed commitments | Privacy Program Owner + Technical Privacy Lead |

| 4 | Legal review for material changes | Legal counsel |

| 5 | Approve: Privacy Program Owner plus Technical Privacy Lead; material changes additionally require CEO approval | Founders |

| 6 | Version the document, record the change in the Change Log with date, author, rationale, and approver | Privacy Program Owner |

| 7 | Notify institutional partners of material changes with advance notice per 14.3 | Privacy Program Owner |

| 8 | Publish and update the effective date | Product Privacy Lead |

| 9 | Retain the superseded version permanently | Privacy Program Owner |

14.2 Material vs. Non-Material Changes

Material changes expand processing, add a data category, add a subprocessor with access to personal data, extend retention, change legal basis, reduce a user right or choice, or alter a disclosed commitment. Material changes require advance notice.

Non-material changes clarify existing language, correct errors, improve readability, or narrow processing. Non-material changes are logged and published without advance notice, though the effective date is always updated.

Where classification is ambiguous, the change is treated as material.

14.3 Advance Notice for Material Changes

Institutional partners receive 30 days advance notice of material changes, delivered directly to the institutional contact of record rather than only by posting. The notice states what is changing, why, what it means for their data, and how to object or escalate. End users are notified in-platform where the change affects their data or choices.

Scholera does not apply a material change retroactively to data already collected without either an applicable legal basis or fresh consent.

14.4 Registers Maintained

| Register | Contents | Owner | Retention |

|---|---|---|---|

| Data Inventory | Per Section 3.4 | Technical Privacy Lead | Current + full version history |

| Privacy Request Register | All individual rights requests and outcomes | Privacy Program Owner | 3 years minimum |

| Legal Process Register | All law enforcement and legal process requests | Privacy Program Owner | Permanent |

| Data Request Register | Institutional and internal data requests | Privacy Program Owner | 3 years minimum |

| Vendor Register | Vendor assessments, DPAs, review dates | Privacy Program Owner | Relationship + 3 years |

| DPIA Register | All completed DPIAs | Privacy Program Owner | Permanent |

| Non-Compliance Register | All privacy non-compliance events | Privacy Program Owner | Permanent |

| Access Review Log | Quarterly production access reviews | Technical Privacy Lead | 3 years minimum |

| Exception Log | Approved deviations from this program | Privacy Program Owner | Permanent |

| Change Log | All changes to this program and the Privacy Policy | Privacy Program Owner | Permanent |

14.5 Annual Program Review

The Privacy Program Owner conducts a full review of this program annually, assessing: accuracy of the data inventory, adequacy of vendor assessments, timeliness of rights request handling, patterns in the Non-Compliance Register, changes in applicable law, and progress against the roadmap in Section 15. Findings and resulting changes are recorded.

14.6 Training

All personnel complete privacy training at onboarding covering: this program's core obligations, the reporting duty under Section 13.2, data handling requirements, the law enforcement escalation rule under Section 6.4, and the internal access rules under Section 10.3. Refresher training is delivered annually and upon material changes to this program.

15. Current Posture and Roadmap

Scholera is an early-stage company. This program describes the framework we operate to, and we are transparent that portions of it are newly formalized rather than long-established. The following is an honest statement of where we stand.

15.1 Implemented

- Architectural privacy controls: data minimization, role-based access scoping, encrypted user identifiers, LLM data boundaries, instructor-controlled content, human oversight at consequential decision points
- Encryption in transit (TLS) and at rest (AES-256)
- Peer review of all code changes with staging validation before production
- Onboarding agreements including confidentiality and security policy acknowledgment
- Privacy contact of record and rights request handling on the timelines in Section 5
- Small, deliberately constrained subprocessor surface

15.2 In Progress

| Item | Target |

|---|---|

| Complete verification of all [VERIFY] entries in the data inventory | Q4 2026 |

| Confirm or execute formal DPAs with all subprocessors | Q4 2026 |

| Cookie consent interface | Q1 2027 |

| Privacy Center with structured request form | Q1 2027 |

| In-platform consent withdrawal controls | Q1 2027 |

| Formal stop-processing and rights request procedure documentation | Q1 2027 |

| Onboarding and offboarding procedure documentation with access checklists | Q1 2027 |

| Published FERPA data processing documentation | Q1 2027 |

| Privacy impact checkpoint formalized in the product development lifecycle | Q2 2027 |

| Formal third-party privacy assessment framework with annual review cycle | Q2 2027 |

| Publicly posted AI governance documentation | Q2 2027 |

| Internal audit framework | Q2 2027 |

| NIST Cybersecurity Framework alignment | Q3 2027 |

| SOC 2 Type I completion | Q3 2027 |

| First transparency report | Q4 2027 |

| SOC 2 Type II initiation | Q4 2027 |

15.3 Known Gaps

We state these plainly rather than leaving an institutional reviewer to discover them:

- Several data inventory entries require technical verification before the inventory can be represented as complete
- Formal DPA status with certain subprocessors requires confirmation; any subprocessor operating under standard rather than enterprise terms is a remediation priority
- Cookie consent mechanism is not yet implemented
- Backup retention behavior needs documentation before deletion timelines can be described precisely
- Internal audit function is not yet formalized
- Third-party library currency and validation process is under development

16. Contact

Scholera Inc.

SCHOLERA

Privacy Program Owner: Pat Roscio, Chief Operating Officer

Email: proscio@scholera-inc.com

Location: New Jersey, United States

Institutional partners with questions about this program, requests for supporting documentation, or concerns about Scholera's privacy practices are encouraged to contact us directly. We treat institutional privacy review as a collaboration rather than a hurdle, and the questions institutional reviewers ask have materially improved this program.