

VIRTUAL RESEARCH INSTITUTE LLC

Privacy, Records Retention and Institutional AI Use Policy

Data minimization, approved systems, human-reviewed AI, retention, deletion, and participant privacy controls

Organization: Virtual Research Institute LLC

Document Type: Privacy, Records Retention and Institutional AI Use Policy

Status: Adopted and Effective

Effective Date: August 20, 2026

Version: Version 1.1

Supersedes: Version 1.0

Applies To: Applicants, students age 13+, families, mentors, contractors, staff, guests, and VRI service providers

Policy Statement. This policy establishes VRI rules for collecting, using, storing, sharing, retaining, deleting, and processing personal, academic, administrative, financial, and program information, including limited use of approved artificial-intelligence systems.

Relationship to Other Documents. The Policies & Procedures Manual and Student Code establish public expectations. The Session Recording Policy governs recordings. The Parent / Guardian Enrollment and Consent Package captures required acknowledgments and optional permissions.

Contents

1. Purpose and Governing Principles
2. Scope
3. Data Categories
4. Collection, Notice, and Minimum Age
5. Approved Systems and Access
6. Permitted Uses
7. Institutional AI and Automated Decision Support
8. Retention Schedule
9. Recording and Derivative Records
10. Public Research Archive and Media
11. Parent and Participant Requests
12. Vendor and Partner Controls
13. Security and Incident Response
14. Roles and Responsibilities
15. Implementation Controls
- Appendix A.** Minimum-Necessary AI Assignment Dataset
- Appendix B.** Standard AI Disclosure
- Appendix C.** AI Systems Registry Requirements

1. Purpose and Governing Principles

- Collect and use the minimum information reasonably necessary for an approved purpose.
- Keep institutional records in VRI-controlled systems with role-based access.
- Use AI only as human-reviewed decision support and never as independent authority for consequential decisions.
- Separate approved one-to-one exception recordings and private symposium recordings from the de-identified Public Research Archive and from any separate optional publicity or media use.
- Delete temporary and obsolete records on a defined schedule unless a preservation hold applies.

2. Scope

This policy applies to applications, registrations, readiness information, assignment data, schedules, communications, payments, academic work, progress records, completion records, certificates, recordings, incident records, mentor records, website submissions, and data processed through VRI-approved vendors or AI systems.

3. Data Categories

3.1 Core Administrative Data

Names, contact information, guardian relationship, date of birth or age, grade level, school status, location, time zone, emergency contacts, and program selections.

3.2 Academic and Program Data

Coursework, skills, readiness responses, project rankings, schedule availability, mentor notes, progress records, contributions, deliverables, completion records, and evaluations.

3.3 Sensitive and Restricted Data

Payment or banking data, government identifiers, detailed health or disability records, background-check information, safeguarding records, incident records, legal correspondence, identity-verification materials, and raw recordings. These records receive the highest access controls and may not be used in ordinary AI workflows.

4. Collection, Notice, and Minimum Age

- VRI will provide understandable notice describing the information collected, purpose, service providers, retention, and request process.
- VRI programs are designed for high school students. Every student must be at least 13 years old when the program begins. VRI does not enroll students under age 13.
- The registration system must conduct an early age check. If the student will be under 13 when the program begins, the registration process must stop before substantive application data, agreements, or payment information are collected.
- VRI does not operate a parental-consent enrollment path for children under age 13. If VRI learns that under-13 information was submitted, access must be restricted and the information reviewed for prompt deletion except for minimum records lawfully needed for security, duplicate prevention, or audit.
- Required program acknowledgments and the Public Research Archive notice must be clearly presented. Any separate publicity or media permission must remain optional and distinct.

5. Approved Systems and Access

- Institutional data must be stored in VRI-approved systems and accounts.
- Access is limited according to role and legitimate business need. High-risk records require stronger restrictions and multi-factor authentication.
- Student or family data may not be copied into personal email, personal cloud storage, consumer messaging applications, personal devices, or unapproved AI accounts.
- VRI maintains an Approved AI Systems Registry. No system may process participant data outside the data categories, account, purpose, and controls recorded in the registry.

6. Permitted Uses

- Application and registration administration.
- Academic-readiness review, schedule compatibility, project fit, and human-approved assignment.
- Program delivery, attendance, communication, academic support, documentation, completion review, and quality assurance.
- Safeguarding, complaint review, incident response, dispute review, legal compliance, insurance, and fraud prevention.
- Payment, refund, accounting, tax, contractor-payment, and reconciliation.
- Approved de-identified Public Research Archive publication under VRI archive rules, and separate publicity or promotional use only when the applicable affirmative permission exists.

7. Institutional AI and Automated Decision Support

7.1 Permitted AI Uses

- Completeness and duplicate checks.
- Readiness triage and identification of records requiring human clarification.
- Schedule compatibility and draft project-assignment recommendations.
- Summarization of minimized, non-sensitive application or academic information.
- Drafting communications, checklists, reports, and internal review notes.

7.2 Human Authority and Review

- AI output is advisory and may not independently admit, reject, discipline, remove, refund, award aid, determine an accommodation, make a safeguarding finding, assign authorship, or publish a record.
- An authorized reviewer must verify source data, assess missing context and bias, and approve the final action.
- The institutional record should retain the final human decision and concise rationale rather than unnecessary raw prompts or outputs.

7.3 Data Preparation

- Use a stable participant ID instead of a name whenever practical.
- Include only fields necessary for the approved purpose.
- Exclude home addresses, personal phone numbers, exact birth dates, payment credentials, detailed health records, identity documents, sensitive incident narratives, and raw recordings from ordinary analysis.
- Use the operational accommodation requirement rather than an underlying diagnosis unless the diagnosis is genuinely necessary.

7.4 Approved AI Environment

- Use only systems listed in the VRI Approved AI Systems Registry and only through the recorded VRI business workspace or approved API configuration.

- The registry must record the vendor, authorized account, permitted and prohibited data, purpose, responsible administrator, retention and training terms reviewed, and date of last review.
- Use ephemeral or temporary session modes where operationally appropriate. Do not upload the master registration workbook. Delete saved files and conversation records when the approved task is complete.
- Review vendor privacy, training, retention, deletion, subprocessors, access, and security terms before approving participant-data use and after material changes.

7.5 Prohibited AI Uses

- Training a general-purpose model on VRI participant records or recordings.
- Facial recognition, biometric identification, emotion analysis, sensitive-trait inference, or synthetic-media creation involving participants.
- Uploading raw recordings, safeguarding files, detailed medical records, payment credentials, identity documents, or background-check reports for ordinary analysis.
- Secret or undisclosed automated decision-making that materially affects a participant or family.

8. Retention Schedule

Record	Retention target
Unsuccessful, incomplete, or withdrawn student applications	18 months after final decision or last substantive contact
Enrollment agreements, acknowledgments, consents, payment and refund records, and core administrative records	7 years after end of calendar year of final participation
Academic progress, contribution, evaluation, and ordinary project working records	3 years after final participation
Approved one-to-one exception recordings	90 days after end of relevant program term
Symposium recordings	3 years after symposium date
Completion verification record	Permanent
Rendered signed certificate artifact	7 years after end of calendar year of final participation
Temporary AI working files, pseudonymous exports, and ordinary AI conversation records containing participant data	Until approved task is complete and normally no later than 30 days after final human decision
Public Research Archive materials	According to the archive schedule and institutional purpose; public copies remain de-identified
Incident, safeguarding, legal, insurance, or investigation records	Restricted matter schedule; never delete during preservation hold

These are VRI operational targets and may be extended by legal, tax, insurance, contractual, safeguarding, or preservation-hold requirements. A verification record is distinct from the certificate artifact and exists so VRI can verify completion and reissue a certificate in the future.

9. Recording and Derivative Records

- Routine Research Circle and Research Team sessions are not recorded.
- Approved one-to-one exception recordings and private symposium recordings are governed by the Session Recording Policy.
- Automatic transcripts and AI summaries are disabled by default. Each derivative creates a new record with its own access and retention controls.

- A purpose-specific exception must define the approved system, users, purpose, fields, retention, deletion date, and notice requirements.

10. Public Research Archive and Media

- Student names and other direct student-identifying information are excluded from the Public Research Archive. Public archive entries may include approved project titles, abstracts, mentor information, topic and term metadata, project summaries, and de-identified scholarly outputs.
- VRI may redact, reformat, excerpt, or withhold an artifact before archive publication when needed to remove student-identifying information or protect privacy, confidentiality, scholarly integrity, or third-party rights.
- Student identity, enrollment, contribution, completion, and certificate records remain in restricted VRI systems and are not published as part of the Public Research Archive.
- Publicity and promotional use of student-identifying material is optional, is separate from the Public Research Archive, and requires a separate applicable affirmative permission.
- Private symposium recording and cohort-family access is not Public Research Archive or publicity use. A publicity permission does not authorize student identity in the Public Research Archive.

11. Parent and Participant Requests

- Verify the requester before providing access to or changing a participant record.
- Requests may include correction, access, restriction, withdrawal of optional publicity or media permission, or deletion where applicable.
- Collaborative records may require a redacted excerpt, supervised review, restricted link, or written summary to protect other participants.
- Withdrawal of optional media or publicity permission generally applies prospectively. Requests concerning Public Research Archive material are handled through VRI correction, redaction, reformatting, and removal procedures; private institutional records remain subject to lawful retention requirements.

12. Vendor and Partner Controls

- Written terms should limit vendor use to the approved purpose, restrict redisclosure, require appropriate security, and address deletion or return of data.
- VRI must document service accounts, access scope, data flows, subprocessors where known, and the person responsible for the relationship.
- A partner's access does not convert VRI records into unrestricted partner data.

13. Security and Incident Response

- Use multi-factor authentication, least privilege, secure sharing, access logs where available, and prompt revocation.
- Report suspected unauthorized access, loss, disclosure, or misuse promptly.
- Document the incident, preserve relevant evidence, restrict access, evaluate notification duties, and implement corrective action.

14. Roles and Responsibilities

- Executive Director: policy authority, vendor and AI-system approval, high-risk exceptions, and final institutional decisions.
- Privacy / Safeguarding Lead: requests, incident review, recording access, preservation holds, and restricted records.

- Operations: acknowledgment records, retention schedules, deletion logs, approved exports, certificate delivery, and audit evidence.
- Mentors and staff: minimum-necessary access, approved systems, prompt reporting, and no personal copies.
- Technology Administrator: account controls, automation, logs, backups, access review, and secure deletion.

15. Implementation Controls

- Maintain the data inventory, system-of-record map, and Approved AI Systems Registry.
- Implement required acknowledgments, the Public Research Archive notice, and any separate optional publicity or media permissions with immutable policy-version references.
- Implement an early 13+ registration gate.
- Implement pseudonymous assignment-export tooling and 30-day AI working-file deletion.
- Implement the 90-day approved-exception recording deletion, 3-year symposium schedule, 7-year certificate artifact schedule, and permanent verification record.
- Publish a parent-facing privacy notice and request process.
- Review this policy after attorney review and after material vendor, platform, or program changes.

Appendix A. Minimum-Necessary AI Assignment Dataset

Participant ID; pathway; grade or academic level; relevant coursework and skills; project rankings; schedule availability; time zone; project prerequisites; operational accommodation requirement where necessary; and reviewer notes limited to academic fit.

Appendix B. Standard AI Disclosure

VRI may use approved business AI tools to assist authorized personnel with limited administrative and academic review, such as completeness checks, readiness triage, schedule analysis, draft assignment recommendations, summarization, and communication drafting. VRI uses minimized or pseudonymous information where practical. AI output is advisory, and authorized VRI personnel make or approve consequential decisions. VRI does not authorize ordinary AI use of raw recordings, payment credentials, detailed health records, identity documents, or sensitive safeguarding files.

Appendix C. AI Systems Registry Requirements

- System and vendor name.
- Authorized VRI account, workspace, project, or API configuration.
- Approved purpose and owner.
- Permitted and prohibited data categories.
- Retention, training, deletion, subprocessors, and access terms reviewed.
- Responsible administrator and date of last review.
- Operational status and any restrictions.