VISTARA VIDYAANIDHI EDUCATIONAL TRUST

DATA PRIVACY AND DATA PROTECTION POLICY

Policy Number: VVET-DPP-006
Effective Date: 09/06/2026
Approved By: Board of Trustees
Policy Owner: Board of Trustees
Review Frequency: Every Three (3) Years or Earlier if Required

1. PREAMBLE

Vistara Vidyaanidhi Educational Trust ("the Trust") recognizes that personal data is an important organizational asset and that individuals have legitimate expectations regarding the privacy, security, confidentiality, and lawful handling of their personal information.

The Trust is committed to protecting the privacy rights of beneficiaries, students, scholarship applicants, parents, guardians, employees, volunteers, interns, donors, trustees, consultants, partners, vendors, service providers, website users, event participants, and all other individuals whose personal information may be collected, processed, stored, transmitted, accessed, disclosed, or otherwise handled by the Trust.

As an educational and charitable institution, the Trust routinely interacts with students, educational institutions, parents, volunteers, donors, community members, researchers, public authorities, corporate partners, and other stakeholders. These interactions may require the collection and processing of personal information in order to deliver programs, administer scholarships, conduct educational activities, manage partnerships, comply with legal obligations, communicate with stakeholders, and fulfill organizational objectives.

The Trust acknowledges its responsibility to manage personal information lawfully, fairly, transparently, securely, and responsibly.

This Data Privacy and Data Protection Policy establishes the principles, standards, responsibilities, safeguards, and governance mechanisms that shall guide the collection, use, storage, disclosure, retention, transfer, protection, and disposal of personal information handled by the Trust.

The Trust is committed to respecting privacy rights while balancing operational, legal, educational, governance, safeguarding, and organizational requirements.

2. PURPOSE OF THE POLICY

The purpose of this Policy is to establish a comprehensive framework for the responsible management of personal information and to ensure that data protection considerations are integrated into the governance, operations, systems, programs, partnerships, and activities of the Trust.

This Policy seeks to:

- Protect personal information from misuse.
- Promote responsible data management practices.
- Strengthen privacy safeguards.
- Reduce data protection risks.
- Support organizational accountability.
- Promote transparency regarding data handling.
- Establish security expectations.
- Support compliance with applicable laws and regulations.
- Protect the rights and interests of data subjects.
- Promote stakeholder confidence.

The Trust recognizes that effective privacy protection contributes to public trust, organizational credibility, and responsible stewardship of information.

3. SCOPE AND APPLICABILITY

This Policy applies to all personal information collected, processed, stored, accessed, transmitted, disclosed, shared, archived, or disposed of by the Trust.

This Policy applies to:

- Trustees;
- Employees;
- Volunteers;
- Consultants;
- Advisors;
- Interns;
- Contractors;
- Vendors;
- Technology service providers;
- Research personnel;
- Partner organizations handling Trust data;

- Any individual acting on behalf of the Trust.

The Policy applies to information handled through:

- Physical records;
- Paper documents;
- Digital systems;
- Websites;
- Mobile applications;
- Email systems;
- Cloud platforms;
- Learning management systems;
- Scholarship portals;
- Databases;
- Audio recordings;
- Video recordings;
- Photographs;
- Communication platforms;
- Social media systems;
- Any other information management system.

The obligations established under this Policy apply regardless of format, location, technology platform, or method of processing.

4. POLICY STATEMENT

The Trust is committed to protecting personal information and ensuring that data processing activities are conducted responsibly, lawfully, ethically, and transparently.

Personal information shall only be collected, accessed, used, disclosed, retained, and disposed of for legitimate organizational purposes.

The Trust shall endeavor to implement reasonable administrative, technical, physical, contractual, and organizational safeguards to protect personal information from unauthorized access, disclosure, alteration, loss, misuse, destruction, or compromise.

Privacy considerations shall be integrated into organizational decision-making and operational practices.

All individuals associated with the Trust share responsibility for protecting personal information.

5. GUIDING PRINCIPLES OF DATA PROTECTION

5.1 Lawfulness and Fairness

The Trust shall endeavor to collect and process personal information through lawful, ethical, and fair means.

Individuals shall not be deceived, misled, manipulated, or improperly pressured into providing personal information.

The Trust shall seek to ensure that data processing activities are consistent with legitimate organizational purposes.

5.2 Transparency

The Trust believes that individuals should understand how their information is collected, used, stored, shared, and protected.

Accordingly, the Trust shall endeavor to communicate relevant privacy information clearly and appropriately.

Transparency promotes trust and informed participation in organizational activities.

5.3 Purpose Limitation

Personal information shall be collected only for legitimate, specified, and relevant purposes.

The Trust shall seek to avoid collecting information that is unnecessary, excessive, unrelated, or disproportionate to the purpose for which it is required.

Information shall not be used for unrelated purposes without appropriate justification or authorization.

5.4 Data Minimization

The Trust shall endeavor to limit data collection to information reasonably necessary for organizational operations and objectives.

The collection of excessive personal information increases privacy risks and shall be avoided.

The Trust recognizes that responsible data management begins with collecting only what is genuinely required.

5.5 Accuracy

The Trust shall endeavor to maintain personal information that is reasonably accurate, relevant, complete, and up to date.

Where inaccuracies are identified, reasonable efforts may be undertaken to correct, update, or clarify information.

Accurate records support effective service delivery, governance, and stakeholder engagement.

5.6 Security

The Trust recognizes that personal information must be protected against unauthorized access, disclosure, misuse, alteration, destruction, theft, or loss.

Reasonable safeguards shall be implemented to support information security and confidentiality.

Security is a shared responsibility applicable to all individuals handling Trust information.

5.7 Accountability

The Trust shall maintain responsibility for information under its control and shall endeavor to establish governance mechanisms that promote compliance with privacy and data protection obligations.

Accountability includes oversight, training, monitoring, risk management, and continuous improvement.

6. DEFINITIONS

For the purposes of this Policy:

Personal Information

Personal information refers to any information that identifies, relates to, describes, concerns, or can reasonably be associated with an identifiable individual.

Examples may include:

- Names;
- Addresses;
- Contact details;
- Email addresses;

- Identification information;
- Educational records;
- Scholarship records;
- Photographs;
- Video recordings;
- Employment records;
- Volunteer information;
- Financial information;
- Communication records.

Data Subject

A data subject refers to the individual to whom personal information relates.

Examples include:

- Students;
- Scholarship applicants;
- Beneficiaries;
- Employees;
- Volunteers;
- Donors;
- Parents;
- Guardians;
- Trustees;
- Vendors.

Processing

Processing includes any activity involving personal information, including:

- Collection;
- Recording;

- Organization;
- Storage;
- Retrieval;
- Consultation;
- Use;
- Analysis;
- Sharing;
- Transmission;
- Disclosure;
- Archiving;
- Deletion;
- Destruction.

7. CATEGORIES OF INFORMATION COLLECTED

The Trust may collect and process various categories of information depending on organizational needs and activities.

Such information may include:

Identity Information

- Full name;
- Date of birth;
- Gender;
- Identification details;
- Photographs.

Contact Information

- Address;
- Phone number;
- Email address;
- Emergency contact details.

Educational Information

- Academic records;
- School information;
- Scholarship applications;
- Certifications;
- Training participation records.

Employment and Volunteer Information

- Applications;
- Qualifications;
- References;
- Experience records;
- Training records.

Financial Information

- Payment information;
- Banking details;
- Scholarship disbursement records;
- Donation records.

Technical Information

- Website usage information;
- Device information;
- Login records;
- System activity logs.

The Trust shall endeavor to collect only information reasonably necessary for legitimate organizational purposes.

8. COLLECTION OF PERSONAL INFORMATION

The Trust may collect information through various methods, including:

- Scholarship applications;
- Registration forms;
- Website submissions;
- Program enrollment;
- Volunteer applications;
- Employment processes;
- Surveys;
- Research activities;
- Events and workshops;
- Donor interactions;
- Partnership activities;
- Communication platforms.

Information may be collected directly from individuals, parents, guardians, educational institutions, authorized representatives, public records, partner organizations, or other lawful sources.

The Trust shall endeavor to ensure that collection methods are transparent, appropriate, and consistent with organizational objectives.

9. CHILDREN'S DATA AND SAFEGUARDING INFORMATION

The Trust recognizes that information relating to children requires heightened protection.

Where programs involve minors, the Trust shall take additional precautions to protect children's personal information.

The Trust shall seek to ensure that:

- Children's information is handled responsibly;
- Access is restricted;
- Safeguarding information remains confidential;
- Media content is managed appropriately;
- Risks to child privacy are minimized.

The protection of children's information shall be treated as a high organizational priority.

10. LEGAL BASIS FOR COLLECTION AND PROCESSING OF PERSONAL INFORMATION

The Trust recognizes that personal information should only be collected, accessed, used, disclosed, retained, transferred, or otherwise processed where there is a legitimate organizational purpose and an appropriate legal, contractual, operational, educational, safeguarding, governance, or regulatory basis for doing so.

The Trust may process personal information for purposes including:

- Administration of educational programs;
- Scholarship management;
- Beneficiary support activities;
- Volunteer management;
- Internship administration;
- Recruitment processes;
- Employee administration;
- Event management;
- Donor engagement;
- Partnership management;
- Compliance activities;
- Research initiatives;
- Safeguarding obligations;
- Financial administration;
- Risk management;
- Legal compliance.

The Trust shall endeavor to ensure that information processing activities remain proportionate, relevant, necessary, and consistent with the purpose for which information was collected.

Personal information shall not be processed in a manner that is incompatible with legitimate organizational objectives or applicable legal requirements.

The Trust shall periodically review processing activities to ensure continued necessity, appropriateness, and accountability.

11. CONSENT

The Trust recognizes that consent may be an important basis for collecting and using personal information in certain circumstances.

Where consent is relied upon, the Trust shall endeavor to ensure that consent is:

- Voluntary;
- Informed;
- Specific;
- Understandable;
- Freely provided;
- Appropriately documented where required.

Individuals should be provided with sufficient information to understand:

- What information is being collected;
- Why information is being collected;
- How information will be used;
- Who may receive the information;
- Any relevant risks associated with disclosure.

The Trust recognizes that consent may not always be the sole basis for processing information. Certain processing activities may be necessary for safeguarding, legal compliance, contractual obligations, organizational administration, educational program delivery, or legitimate organizational interests.

Where children are involved, the Trust may seek parental, guardian, institutional, or other legally appropriate authorization where required.

12. USE OF PERSONAL INFORMATION

The Trust shall use personal information only for legitimate and authorized purposes consistent with organizational objectives.

Personal information may be used for:

Program Administration

Including:

- Educational activities;
- Scholarship administration;

- Student support;
- Training programs;
- Certification activities;
- Mentorship initiatives.

Organizational Operations

Including:

- Human resource management;
- Volunteer administration;
- Financial management;
- Governance activities;
- Risk management;
- Compliance requirements.

Communication

Including:

- Program updates;
- Event notifications;
- Scholarship communication;
- Volunteer engagement;
- Stakeholder communication.

Monitoring and Evaluation

Including:

- Program assessment;
- Research activities;
- Impact measurement;
- Reporting requirements.

Legal and Regulatory Compliance

Including:

- Audit requirements;
- Government reporting;
- Regulatory obligations;
- Court orders;
- Investigations.

The Trust shall endeavor to ensure that information is not used for unauthorized, deceptive, discriminatory, exploitative, or unlawful purposes.

13. DATA SHARING AND DISCLOSURE

The Trust recognizes that certain activities may require the sharing or disclosure of information with authorized parties.

Information may be disclosed where:

- Necessary for program delivery;
- Required by law;
- Required for safeguarding purposes;
- Necessary for audits;
- Required by funding agreements;
- Required by educational partnerships;
- Necessary for operational activities.

Potential recipients may include:

- Educational institutions;
- Government agencies;
- Regulatory authorities;
- Auditors;
- Service providers;
- Technology providers;
- Donors and funding agencies;
- Research partners;

- Legal advisors.

The Trust shall endeavor to limit disclosures to information reasonably necessary for the intended purpose.

Unauthorized disclosure of personal information is prohibited.

The Trust shall seek to ensure that recipients of personal information are capable of handling information responsibly and appropriately.

14. THIRD-PARTY SERVICE PROVIDERS

The Trust may engage external vendors, consultants, technology providers, cloud service providers, software providers, educational partners, event organizers, auditors, legal advisors, and other service providers who may have access to personal information.

The Trust shall endeavor to take reasonable steps to ensure that third parties:

- Protect personal information appropriately;
- Maintain confidentiality;
- Use information only for authorized purposes;
- Implement appropriate security measures;
- Comply with applicable obligations.

Third parties shall not be permitted to use personal information for their own unrelated commercial purposes without appropriate authorization.

The Trust reserves the right to review, monitor, and assess third-party data protection practices where appropriate.

15. DATA SECURITY AND INFORMATION PROTECTION

The Trust recognizes that protecting personal information requires a combination of administrative, technical, physical, and organizational safeguards.

Accordingly, the Trust shall endeavor to implement reasonable security measures designed to prevent:

- Unauthorized access;
- Unauthorized disclosure;
- Accidental loss;
- Theft;

- Misuse;
- Alteration;
- Destruction;
- Corruption of information.

Security measures may include:

Administrative Controls

- Policies and procedures;
- Training and awareness programs;
- Access management;
- Authorization processes.

Technical Controls

- Password protection;
- Authentication systems;
- Encryption technologies;
- Network security measures;
- Backup systems.

Physical Controls

- Secure storage;
- Controlled facility access;
- Visitor management procedures;
- Secure disposal mechanisms.

The Trust recognizes that no security system is entirely risk-free; however, reasonable efforts shall be undertaken to protect information under its control.

16. ACCESS CONTROL

Access to personal information shall be limited to individuals who require such access for legitimate organizational purposes.

The Trust shall seek to implement appropriate access control mechanisms to ensure that information is only available to authorized personnel.

Access permissions may be determined based on:

- Job responsibilities;
- Program requirements;
- Operational needs;
- Safeguarding considerations;
- Governance responsibilities.

Individuals shall not access, review, copy, modify, disclose, or use information beyond the scope of their authorized responsibilities.

Unauthorized access to information may constitute a serious violation of organizational policy.

17. CONFIDENTIALITY OBLIGATIONS

Individuals who have access to personal information are expected to maintain strict confidentiality.

Confidential information shall not be disclosed to unauthorized individuals or entities.

Confidentiality obligations apply to:

- Trustees;
- Employees;
- Volunteers;
- Consultants;
- Interns;
- Contractors;
- Service providers.

The obligation to protect confidential information continues even after an individual's association with the Trust ends.

Confidential information shall only be disclosed where authorized, legally required, or necessary to protect individuals or organizational interests.

18. RETENTION OF PERSONAL INFORMATION

The Trust recognizes that information should not be retained indefinitely without legitimate justification.

Personal information shall be retained only for as long as reasonably necessary to:

- Fulfill organizational purposes;
- Meet legal obligations;
- Support audits;
- Resolve disputes;
- Maintain records;
- Comply with regulatory requirements.

Retention periods may vary depending on the type of information involved.

The Trust shall periodically review retained information and may dispose of information that is no longer required.

19. SECURE DISPOSAL OF INFORMATION

When personal information is no longer required, the Trust shall endeavor to dispose of information securely and responsibly.

Secure disposal measures may include:

Physical Records

- Shredding;
- Secure destruction;
- Controlled disposal.

Electronic Records

- Secure deletion;
- Data wiping;
- Destruction of storage media.

The objective of secure disposal is to prevent unauthorized access to information after it is no longer needed.

20. DATA BREACHES AND SECURITY INCIDENTS

The Trust recognizes that despite reasonable safeguards, security incidents may occur.

A data breach may include:

- Unauthorized access;
- Unauthorized disclosure;
- Loss of information;
- Theft of records;
- Accidental disclosure;
- Cybersecurity incidents;
- System compromise.

Individuals who become aware of actual or suspected breaches shall report them promptly through appropriate channels.

The Trust shall endeavor to:

- Assess the incident;
- Contain risks;
- Protect affected individuals;
- Investigate causes;
- Implement corrective measures;
- Fulfill legal or regulatory obligations.

Prompt reporting is critical to effective incident management.

21. CYBERSECURITY RESPONSIBILITIES

All individuals using organizational technology systems share responsibility for protecting information assets.

Individuals shall:

- Protect passwords;
- Use authorized software;
- Report suspicious activities;
- Follow security procedures;

- Avoid sharing credentials;
- Exercise caution with emails and links.

The Trust prohibits:

- Unauthorized system access;
- Circumvention of security controls;
- Distribution of malicious software;
- Unauthorized data extraction;
- Misuse of technology resources.

Cybersecurity awareness forms an important component of information protection.

22. RIGHTS OF DATA SUBJECTS

The Trust recognizes that individuals whose personal information is collected, processed, stored, or otherwise handled by the organization have legitimate interests regarding the management of their personal information.

Subject to applicable laws, regulatory obligations, safeguarding requirements, contractual obligations, organizational needs, and legitimate limitations, individuals may have the right to:

- Request access to their personal information;
- Request correction of inaccurate information;
- Request updating of incomplete information;
- Request clarification regarding information processing activities;
- Request withdrawal of consent where consent is the basis of processing;
- Request deletion of information where appropriate;
- Request restriction of certain processing activities;
- Raise concerns regarding privacy practices;
- Submit complaints relating to personal information.

The Trust shall endeavor to review and respond to requests within a reasonable period of time.

The exercise of individual rights may be subject to limitations where information is required for:

- Legal obligations;
- Regulatory compliance;

- Safeguarding purposes;
- Contractual requirements;
- Investigations;
- Governance responsibilities;
- Protection of organizational interests.

The Trust shall balance privacy rights with other legitimate responsibilities and obligations.

23. CHILDREN'S PRIVACY AND PROTECTION OF MINORS' INFORMATION

The Trust recognizes that children require enhanced privacy protection and special safeguards regarding the collection, use, disclosure, storage, and management of personal information.

The Trust shall exercise particular care when handling information relating to:

- School students;
- Scholarship applicants who are minors;
- Competition participants;
- Training participants;
- Beneficiaries below the age of eighteen;
- Child safeguarding cases.

The Trust shall endeavor to:

- Minimize collection of children's information;
- Restrict access to authorized personnel;
- Protect educational records;
- Safeguard identity information;
- Protect photographs and media content;
- Prevent unnecessary disclosure.

The Trust recognizes that privacy protection forms an integral component of child safeguarding.

Information relating to child protection concerns, safeguarding reports, investigations, welfare matters, or sensitive personal circumstances shall receive enhanced confidentiality protections.

No individual shall disclose information relating to a child without appropriate authorization, legal basis, or safeguarding justification.

24. PHOTOGRAPHY, VIDEOGRAPHY, AND MEDIA CONSENT

The Trust recognizes that photographs, videos, recordings, interviews, testimonials, educational content, promotional materials, and event documentation may involve personal information.

The Trust shall endeavor to ensure that media activities are conducted responsibly and respectfully.

Where appropriate, the Trust may seek consent from:

- Participants;
- Parents or guardians;
- Educational institutions;
- Authorized representatives.

The Trust shall seek to ensure that photographs and recordings:

- Respect individual dignity;
- Avoid exploitation;
- Do not create safeguarding risks;
- Do not expose sensitive information;
- Are consistent with organizational values.

The Trust shall not knowingly use images or recordings in a manner that is misleading, harmful, discriminatory, degrading, exploitative, or inconsistent with the rights and interests of individuals.

Particular care shall be exercised when media content involves children.

25. WEBSITE PRIVACY, DIGITAL PLATFORMS, AND COOKIES

The Trust may operate websites, scholarship portals, registration platforms, educational systems, learning management systems, communication platforms, and other digital services.

Such systems may collect information including:

- Contact information;
- Registration details;
- User activity information;
- Device information;

- Login records;
- Website usage statistics.

The Trust may use cookies or similar technologies to:

- Improve website functionality;
- Enhance user experience;
- Maintain security;
- Analyze website performance;
- Support service delivery.

Individuals may have the ability to manage cookie settings through their browser or device settings.

The Trust shall endeavor to ensure that digital platforms are operated responsibly and in a manner consistent with privacy obligations.

26. INTERNATIONAL AND CROSS-BORDER DATA TRANSFERS

The Trust may utilize technology platforms, cloud services, educational systems, communication services, software providers, or operational partners that process information across different jurisdictions.

Where personal information is transferred, stored, accessed, processed, or managed outside the primary jurisdiction of the Trust, reasonable measures shall be undertaken to promote appropriate protection of personal information.

The Trust shall endeavor to consider:

- Security practices;
- Contractual protections;
- Privacy obligations;
- Safeguarding requirements;
- Organizational risk assessments.

Cross-border data activities shall be conducted responsibly and with due regard for privacy considerations.

27. PRIVACY BY DESIGN AND RISK MANAGEMENT

The Trust recognizes that privacy protection is most effective when incorporated into organizational activities from the outset rather than addressed after risks emerge.

Accordingly, privacy considerations shall be integrated into:

- Program design;
- Scholarship systems;
- Research initiatives;
- Technology deployments;
- Digital platforms;
- Partnership arrangements;
- Data collection processes;
- Operational activities.

The Trust shall endeavor to identify and mitigate privacy risks proactively.

Risk management activities may include:

- Privacy reviews;
- Security assessments;
- Access control evaluations;
- Vendor reviews;
- Compliance monitoring.

The objective is to strengthen protection while supporting organizational effectiveness.

28. AUDITS, REVIEWS, AND COMPLIANCE MONITORING

The Trust recognizes the importance of periodic oversight and assessment of privacy practices.

Accordingly, the Trust may conduct:

- Internal reviews;
- Compliance assessments;
- Security audits;
- Technology evaluations;
- Governance reviews;

- Vendor assessments;
- Risk assessments.

The purpose of such reviews is to:

- Evaluate compliance;
- Identify weaknesses;
- Improve safeguards;
- Strengthen governance;
- Support accountability.

Individuals associated with the Trust shall cooperate with legitimate review and audit activities.

29. INVESTIGATION OF PRIVACY CONCERNS

The Trust reserves the right to investigate concerns relating to:

- Unauthorized access;
- Improper disclosure;
- Security incidents;
- Policy violations;
- Misuse of information;
- Technology misuse;
- Privacy complaints.

Investigations shall be conducted fairly, objectively, confidentially, and in accordance with principles of natural justice.

The Trust may engage:

- Legal advisors;
- Auditors;
- Cybersecurity professionals;
- Technology experts;
- Regulatory authorities;
- Independent investigators.

Individuals shall cooperate with legitimate investigations and provide accurate information.

30. POLICY VIOLATIONS

Violations of this Policy may include:

- Unauthorized access to information;
- Improper disclosure;
- Sharing confidential information;
- Failure to protect records;
- Misuse of personal information;
- Breach of confidentiality obligations;
- Circumvention of security controls;
- Unauthorized data extraction;
- Failure to report security incidents;
- Improper disposal of information.

The Trust treats privacy and information security obligations seriously and expects all individuals to comply with established requirements.

31. DISCIPLINARY ACTION

Violations of this Policy may result in corrective, administrative, contractual, governance, disciplinary, civil, or legal action.

Depending upon the circumstances, actions may include:

- Counseling;
- Training;
- Written warnings;
- Restriction of access privileges;
- Suspension of responsibilities;
- Removal from projects;
- Termination of volunteer engagement;
- Termination of employment;

- Termination of contracts;
- Recovery of losses;
- Reporting to regulators;
- Legal proceedings.

The Trust shall consider the seriousness of the violation, intent, impact, legal obligations, and organizational interests when determining appropriate action.

32. BOARD OVERSIGHT RESPONSIBILITIES

The Board of Trustees bears ultimate responsibility for ensuring that appropriate privacy and data protection governance mechanisms exist within the organization.

The Board shall endeavor to:

- Promote privacy awareness;
- Support information security initiatives;
- Monitor significant privacy risks;
- Review major incidents;
- Support compliance activities;
- Promote responsible information management.

The Board recognizes that privacy protection is an essential component of organizational accountability, stakeholder trust, safeguarding, and governance.

33. GOVERNANCE DECLARATION

The Board of Trustees of Vistara Vidyaanidhi Educational Trust affirms its commitment to protecting the privacy, confidentiality, dignity, and rights of individuals whose information is entrusted to the organization.

The Board recognizes that personal information must be managed responsibly and that privacy protection contributes directly to stakeholder confidence, organizational integrity, safeguarding, legal compliance, and effective governance.

Every individual associated with the Trust shares responsibility for protecting personal information and upholding the principles established under this Policy.