teachSTEM Privacy and Data Protection Policy

Version 2.0 | January 2026

1. Purpose and scope

The purpose of this document is to outline how teachSTEM responsibly collects, stores, uses, and shares data involving children and young people across all programs, school partnerships, citizen science activities, public events, and digital platforms. This policy ensures that teachSTEM protects the rights, privacy, and wellbeing of participants, particularly minors, and avoids unintended legal, ethical, or reputational risks.

This policy has been developed to ensure compliance with the Australian Privacy Act 1988, the Modern Slavery Act 2018 (Cth), and anticipated legislative changes such as the Children's Online Privacy Code. While teachSTEM is not legally required to report under the Modern Slavery Act due to its revenue threshold, the principles embedded in the Act reflect broader community expectations around ethical conduct, transparency, and the protection of children from exploitation. This includes recognising that children's data, particularly when it has economic, research, or policy value, must not be collected, used, or shared in ways that resemble unpaid labour or contribute to commercial gain without safeguards.

Additionally, this policy is informed by child labour legislation and the National Principles for Child Safe Organisations, which mandate that all activities involving children be educational, voluntary, and developmentally appropriate. It recognises that any activity that is coercive, interferes with a child's wellbeing or schooling, or leads to exploitation of their efforts or data is in breach of both national standards and community trust.

This document is also a practical resource for staff, contractors, and partners, helping them understand their responsibilities, apply child-safe and privacy-conscious practices in all data-related activities, and embed ethical considerations into program design and delivery. It ensures that teachSTEM's mission to advance education and environmental sustainability through citizen science is fulfilled in a way that protects and empowers young participants.

2. Guiding Principles

teachSTEM operates on the fundamental belief that children and young people have the right to participate in educational and community-based activities in a safe, respectful, and empowering environment. Our privacy and data protection policy is built on the following guiding principles.

2.1 Protection of Rights and Privacy

We prioritise the dignity, safety, and autonomy of all participants, especially minors. This includes taking active steps to safeguard personally identifiable information, respecting each individual's right to privacy, and upholding protections in line with the Privacy Act 1988 and child safeguarding legislation. We view privacy not simply as compliance, but as a foundational element of child protection and ethical engagement.

2.2 Transparency and Fairness

teachSTEM is committed to open and honest communication with participants, their families, schools, and partner organisations about how and why data is collected, used, stored, and shared. We will ensure that participants understand the purpose of their involvement and are not unknowingly contributing to activities they cannot meaningfully consent to.

2.3 Embedded Consent and Privacy by Design

Privacy and consent are not afterthoughts in our programs, they are integral to how we design, deliver, and evaluate every aspect of our work. We adopt a 'privacy by design' approach, ensuring that systems, forms, consent procedures, and digital tools are created with safeguards in place from the outset. This includes providing clear, age-appropriate explanations and securing informed consent from parents or guardians.

2.4 Proportionate and Purposeful Data Collection

Data will only be collected where it directly supports our educational and research mission. We limit collection to the minimum necessary to achieve defined, transparent purposes. We reject any data practices that resemble surveillance, commercial exploitation, or unnecessary profiling of children.

2.5 Equity and Accountability

Our programs aim to benefit all participants equitably. Where data is used to inform policy, research, or innovation, we commit to ensuring that benefits flow back to the communities and students who contributed. We are accountable to the students, families, schools, and communities we work with, and we will maintain systems to monitor, review, and continuously improve our data protection practices.

3. Legal and Ethical Foundations

teachSTEM's approach to data collection and child engagement is grounded in a firm commitment to both legal compliance and ethical responsibility. We acknowledge that educational initiatives involving children require rigorous standards of safety, transparency, and accountability.

3.1 Relevant Legal Frameworks

Our data and child protection policies are guided by, and seek to align with, the following key legislative instruments:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) – govern the collection, storage, use, and disclosure of personal information in Australia, including expectations around consent, security, and data minimisation.

- Modern Slavery Act 2018 (Cth) – sets community expectations around ethical labour practices. While teachSTEM does not meet the reporting threshold, we voluntarily adopt its principles to ensure that participation in our programs never resembles unpaid labour or commercial exploitation.
- Children's Online Privacy Code (forthcoming) – teachSTEM aligns with the anticipated requirements of this new Code, including heightened protections for online data collected from or about children.
- National Principles for Child Safe Organisations – a framework endorsed by the Council of Australian Governments, which underpins our child protection and ethical engagement standards.

3.2 Ethical Safeguards

We require informed, written consent from a parent or guardian before children or youth engage in any teachSTEM activity involving data collection. Age-appropriate explanations are provided to ensure students also understand:

- What data they are collecting or sharing.
- Why the data matters and how it will be used.
- Their right to say no, ask questions, or withdraw at any time without penalty.

3.3 Privacy and Anonymity

Any personally identifiable information gathered from students is:

- Collected only when essential and with consent.
- Anonymised or de-identified at the earliest opportunity.
- Stored securely and only accessible to authorised personnel.

teachSTEM does not sell or monetise student data. Where data is shared for public good (e.g., through citizen science projects), it is only done in anonymised form and with full transparency to families and schools.

3.4 Non-Exploitation

Where student-generated data contributes to outcomes of potential economic value (e.g. environmental datasets, infrastructure insights, or technology pilots), we:

- Avoid any commercial use without community benefit.
- Reinvest or share insights equitably with students, schools, and local communities.
- Treat students as contributors to learning and change, not unpaid labour.

3.5 Alignment with Education Systems

teachSTEM programs are designed in partnership with schools to:

- Fit within existing curriculum frameworks and teacher-led learning.
- Complement rather than compete with formal education.
- Support student wellbeing, engagement, and age-appropriate development.

4. Data Collection and Usage Practices

teachSTEM engages children and young people in science-based learning programs that often include the collection of observational or environmental data. These practices are designed to foster education, not exploitation, and are implemented with strict safeguards to ensure safety, privacy, and equity.

4.1 Purpose of Data Collection

Data collection within teachSTEM programs is undertaken for the following reasons:

- To promote STEM learning and environmental awareness through hands-on engagement.
- To help students build technical skills in observation, measurement, geolocation, and digital data recording.
- To contribute to public good initiatives, such as citizen science programs that inform environmental planning, biodiversity monitoring, or community services.

All data collection is framed as a curriculum-aligned learning activity rather than labour, research assistance, or commercial content generation.

4.2 Child Participation Requirements

Participation by children in any data collection activity must meet the following conditions:

- Involvement is voluntary and no student will be required to participate. Informed consent from a parent or legal guardian is mandatory and must be documented. Student assent is also required in an age-appropriate format.
- Data activities are linked to learning outcomes and pedagogical goals. They are positioned as experiential learning tools, not performance tasks or outputs with commercial objectives.
- Tools, digital platforms, and activities must be suitable for the cognitive and emotional development of the target age group. Participation must never compromise safety or wellbeing.
- Students' identities, opinions, and creative contributions are acknowledged and protected. Diversity, inclusion, and voice are core to our engagement.

4.3 Types of Data Collected

teachSTEM may facilitate the collection of:

- Environmental observations (e.g. weather, water quality, animal sightings).
- Location-based records (e.g. using GPS or digital maps, anonymised where needed).
- Responses or reflections via guided learning tools or citizen science platforms.

Personal data, including names, photographs, or any identifiers, is only collected if:

- It is essential to the learning activity.
- Proper consent is obtained.
- Storage and usage follow data minimisation principles.

4.4 Data Storage

- All collected data is stored on secure, access-restricted platforms compliant with Australian privacy laws.
- Data is anonymised or pseudonymised unless identifiable information is necessary and clearly consented to.
- Data access is restricted to authorised personnel only, and access is reviewed regularly.

Where data is shared externally (e.g. with research institutions, government partners, or community groups), it must:

- Be de-identified.
- Be accompanied by a plain-language statement explaining its purpose and destination.
- Only be shared for purposes aligned with the public good, such as environmental management or educational evaluation.

4.5 Restrictions on Commercial Use

teachSTEM does not monetise data collected by or about students. If any project or partner proposes using student-generated data in a context where commercial or economic value may be derived, teachSTEM will ensure:

- Community benefit is prioritised, such as reinvestment into participating schools or open access to findings.
- Transparency with families and schools about the potential value and use of data.
- Safeguards against exploitation, in line with child labour and privacy laws.

4.6 Data Access and Use

teachSTEM limits access to personal and sensitive data to authorised personnel only. Access is granted strictly for legitimate program delivery, evaluation, or communication purposes, and in accordance with the roles and responsibilities outlined in this policy.

Data may only be accessed, used, or shared under the following conditions:

- Informed Consent has been provided by the child and/or their parent or guardian.
- Data is de-identified wherever possible to protect privacy, particularly when used for research, reporting, or public dissemination.
- Formal agreements or contracts are in place with any third-party partners, outlining responsibilities for data handling, security, and ethical use.
- Access is limited to a need-to-know basis, with clear records of who accessed the data, when, and for what purpose.

teachSTEM maintains strict controls and audit processes to ensure that all use of data aligns with our mission, protects participant rights, and complies with applicable privacy and child protection laws.

4.7 Rights and Corrections

Participants, or their parents/guardians in the case of minors, have the right to:

- Access the personal information held about them at any time, subject to verification procedures.
- Request corrections to any inaccurate or incomplete data.
- Request deletion of their personal data where appropriate, unless retention is required for legal, safeguarding, or program reporting obligations.

teachSTEM is committed to responding to such requests in a timely, respectful, and lawful manner.

5. Data Sharing and Third-Party Agreements

teachSTEM collaborates with a range of partners, including schools, universities, libraries, citizen science platforms, community organisations, and digital tool providers, to deliver its programs. In all partnerships, data sharing is governed by strict principles that ensure children's privacy, safety, and rights are never compromised.

5.1 Principles of Responsible Data Sharing

Data generated or collected through teachSTEM activities may be shared with third parties only when:

- There is a clear educational or public benefit, such as improving environmental understanding or contributing to community development.
- All personally identifiable information has been removed or anonymised, unless explicit, documented consent has been obtained.

- The receiving party agrees to not re-identify, monetise, or exploit the data in any way that could harm or disadvantage children or their communities.
- The sharing aligns with the Australian Privacy Principles and the best interests of the child, as outlined in the National Principles for Child Safe Organisations.

5.2 Types of Permitted Partners

Permitted data recipients may include:

- Schools or school systems participating in collaborative evaluation or curriculum reporting.
- Research institutions or government bodies analysing trends in education, environmental sustainability, or community engagement.
- Citizen science platforms where data contributes to public knowledge (e.g. biodiversity, climate, or land use studies), provided strong privacy protections are in place.
- Funders or partners requiring program-level (not personal) data to evaluate impact.

All external use must be:

- Non-commercial, or
- Clearly disclosed, with a model for community return or reinvestment.

5.3 Third-Party Agreements and Safeguards

All third parties must sign a Data Access and Use Agreement that outlines:

- Permitted uses of the data (e.g. research, reporting, public education).
- Data security responsibilities, including storage, encryption, access control, and breach reporting.
- Obligations to delete or return data at the end of a project or partnership.
- Prohibitions on profiling, commercial resale, advertising, or marketing based on the data.

If a third party fails to comply, teachSTEM reserves the right to:

- Revoke access immediately.
- Report the breach to relevant authorities or regulatory bodies.
- Notify families or schools as required under the Notifiable Data Breaches Scheme.

5.4 Transparency with Participants

Students, guardians, and schools must be:

- Informed of any external data use at the time of consent.
- Given the option to opt out of any data sharing arrangement that goes beyond the core educational or public benefit scope.

- Provided with plain-language explanations of who has access to their data, why, and how it will be protected.

6. Roles and Responsibilities

To ensure that data collection, storage, use, and sharing are conducted ethically, lawfully, and safely, particularly in the context of programs involving children and young people, specific roles and responsibilities have been defined across the teachSTEM organisation and its partners.

6.1 All Staff, Volunteers, and Contractors

All personnel involved in the design, delivery, or support of teachSTEM activities are responsible for:

- Understanding and complying with this Privacy and Data Protection Policy.
- Completing training on child safety, privacy, and data ethics before participating in any child-facing program.
- Collecting only the minimum data necessary to fulfil program objectives, and ensuring it is used only for the purposes for which consent was given.
- Ensuring that any communication with or about children is respectful, age-appropriate, and non-exploitative.
- Reporting any privacy concerns, misuse of data, or suspected breaches to the Privacy Officer immediately.

6.2 Program and Project Leads

Those responsible for the implementation of teachSTEM programs (e.g., workshops, citizen science initiatives, research partnerships) must:

- Design activities in a way that prioritises privacy, consent, and educational framing.
- Ensure that informed consent forms (including parent/guardian consent where applicable) are obtained, stored securely, and reviewed regularly.
- Maintain clear documentation of how data will be collected, used, and shared.
- Collaborate with schools and communities to ensure that activities do not interfere with education or well-being, and are fully voluntary.

6.3 Privacy and Data Protection Officer

The designated Privacy Officer is responsible for:

- Maintaining and updating this policy in accordance with the Australian Privacy Act, Modern Slavery Act, and emerging regulations such as the Children's Online Privacy Code.
- Providing training, resources, and support to staff and partners on privacy and data ethics.

- Conducting audits and compliance checks on data practices across programs.
- Managing all data breach notifications, including investigations and reporting to the Office of the Australian Information Commissioner (OAIC) where applicable.
- Serving as the point of contact for families, schools, and partners with questions or concerns about privacy or data use.

6.4 Partner Organisations and Third Parties

All external parties receiving or accessing data must:

- Sign formal agreements outlining data use, storage, and deletion protocols.
- Follow all privacy, consent, and security requirements outlined in this policy.
- Be transparent about any further data processing or analysis, and involve teachSTEM in any significant data decisions.
- Report any data breaches or concerns immediately to teachSTEM.

6.5 Schools and Educators

School partners are integral to the ethical implementation of teachSTEM programs. They are encouraged to:

- Actively engage in the co-design of programs to ensure alignment with curriculum, learning outcomes, and school privacy policies.
- Support the distribution and explanation of consent materials to students and families.
- Monitor student participation to ensure it remains voluntary and educationally meaningful.
- Inform teachSTEM of any school-level policies or considerations that may affect data collection or student engagement.

7. Consent and Communication with Children and Families

7.1 Informed Consent

teachSTEM ensures that all participation in its programs, especially those involving data collection by or about children, is underpinned by voluntary, informed consent. This includes:

- For any activity involving children under the age of 18, written consent must be obtained from a parent or legal guardian prior to participation.
- In addition to guardian consent, children must be given age-appropriate explanations of the activity and asked for their assent. Participation must be voluntary, with the option to withdraw at any time.
- Consent forms and supporting information must clearly explain:
    - What data is being collected and why

- How the data will be used, stored, and shared
- Who will have access to the data
- What benefits, if any, the participants and their communities may receive
- What risks, if any, are involved and how they are being managed.

7.2 Age-Appropriate Communication

teachSTEM is committed to using accessible, inclusive, and age-appropriate language in all its communication with children and families, ensuring that:

- Children understand what they are being asked to do and why.
- Guardians are confident that their child's privacy, safety, and wellbeing are prioritised.
- Materials are available in multiple formats or languages if needed to support understanding across diverse communities.

7.3 Ongoing Communication

Consent is not a one-off transaction but part of an ongoing ethical relationship. teachSTEM therefore:

- Keeps families informed about the progress, outcomes, or changes in the program where relevant.
- Provides opt-out options and pathways for families to withdraw consent at any stage.
- Offers open channels of communication, including contact details for the Privacy Officer, to ask questions or raise concerns.

7.4 Special Considerations for Public-Facing Platforms

Where student work, images, voice recordings, or data may be published on websites, social media, or in public-facing reports:

- Separate, specific consent will be obtained outlining the nature of the publication.
- Children and families will be given the choice to participate anonymously or opt out of public-facing content.
- Content will be reviewed to ensure it does not compromise a child's safety, identity, or dignity.

7.5 Informed Participation in Citizen Science and Data Projects

When students are participating in citizen science or environmental data projects:

- The educational framing will be emphasised in all consent materials.

- Schools and families will be briefed on how the project aligns with curriculum and learning outcomes.
- The non-commercial, public-good orientation of the activity will be made clear, unless otherwise stated and approved with safeguards in place.

8. Data Security and Retention

teachSTEM is committed to ensuring that all personal and sensitive information is securely collected, stored, managed, and disposed of in accordance with best practice, ethical standards, and Australian legislation.

8.1 Data Security Measures

To prevent loss, misuse, unauthorised access, or disclosure of data, teachSTEM implements layered, fit-for-purpose security protocols across its systems, which include:

- Digital Security:
    - Use of password-protected and encrypted systems for storing all personal data
    - Access restrictions based on role (i.e. only authorised personnel can access sensitive or identifiable data)
    - Regular audits of digital systems to identify vulnerabilities and ensure compliance with privacy standards.
- Physical Security:
    - Hard copies of documents containing personal or sensitive data are stored in locked cabinets
    - Access to office spaces where sensitive data is handled is restricted and monitored.
- Staff Access and Use:
    - All staff, volunteers, and contractors receive training on privacy obligations and data handling protocols
    - A breach response plan is in place and reviewed regularly in accordance with the Notifiable Data Breaches Scheme under the Privacy Act 1988 (Cth).

8.2 Data Retention

teachSTEM retains personal data only for as long as it is necessary to fulfil the educational, evaluative, or legal purposes for which it was collected.

- Data is only kept if it continues to support the purpose for which it was collected or if legally required.
- Retention Periods:

- Student and parent contact details are deleted at the end of each school year, unless explicitly requested otherwise.
- De-identified data used for research, evaluation, or reporting may be retained longer, in accordance with ethics approvals and privacy protocols.

8.3 Data Disposal and Deletion

When data is no longer required, teachSTEM ensures its secure destruction or deletion.

- Digital data is permanently deleted from all cloud-based and local storage platforms, including backups where possible.
- Physical data is securely shredded or destroyed using confidential disposal services.

8.4 Data Breaches and Incident Management

In the event of a suspected or confirmed data breach:

- teachSTEM will act promptly to contain the breach and assess its severity.
- Affected individuals (including schools, students, and families) will be notified if there is a risk of serious harm.
- The Office of the Australian Information Commissioner (OAIC) will be informed in accordance with the Notifiable Data Breaches (NDB) scheme.

9. Data Breach Management

teachSTEM is committed to the timely identification, containment, and resolution of any incidents involving unauthorised access to, or loss of, personal data. This includes data collected from children, families, schools, or partner organisations.

9.1 Reporting and Notification

All staff, contractors, and volunteers must immediately report any actual or suspected data breach to the designated Privacy Lead. A breach may include:

- Loss or theft of devices containing personal data
- Unauthorised access to program databases or platforms
- Accidental disclosure of personal information to unintended recipients
- Inappropriate sharing of identifiable student or community data.

9.2 Assessment and Response

The Privacy Lead will conduct a swift assessment to determine:

- The nature and scope of the breach

- The type of information involved
- The risk to individuals, especially children
- Whether notification is legally required.

Corrective measures may include:

- Revoking access permissions
- Re-securing systems and platforms
- Updating privacy protocols
- Retraining relevant personnel.

9.3 Notification of Affected Parties

If the breach is assessed as likely to cause serious harm, affected individuals (or their guardians) will be notified in clear, accessible language. The notice will include:

- A description of the breach
- What data was affected
- What steps teachSTEM is taking
- How individuals can protect themselves.

9.4 Reporting to Authorities

Significant breaches will be reported to the Office of the Australian Information Commissioner (OAIC) in accordance with the *Notifiable Data Breaches (NDB) scheme* under the Privacy Act 1988 (Cth).

9.5 Documentation and Review

All breaches, regardless of severity, will be logged and reviewed to strengthen internal systems and avoid recurrence. Outcomes and lessons learned will be shared with relevant stakeholders as appropriate.

10. Monitoring, Review, and Continuous Improvement

teachSTEM is committed to regularly reviewing and refining our privacy and data protection practices to ensure they remain ethical, legally compliant, and responsive to the evolving needs of children, educators, families, and communities.

10.1 Ongoing Monitoring

- We periodically review internal data handling processes to ensure compliance with this policy, including digital security protocols, consent documentation, and data storage practices.
- Teachers, students, families, and staff are encouraged to provide feedback on how personal data is collected, used, and shared. This feedback informs continuous improvement.
- All privacy concerns or breaches (actual or near misses) are recorded, investigated, and used to inform future practice.

10.2 Policy Review Cycle

This policy is formally reviewed at least once per year, or earlier if there are:

- Changes to relevant legislation (e.g. Australian Privacy Act, Children's Online Privacy Code)
- Updates to ethical guidelines or best-practice standards
- Material changes to the nature of teachSTEM programs or data collection activities.

Reviews may involve consultation with:

- Child protection experts
- Educators and school partners
- Data governance advisors
- Students and families (where appropriate).

10.3 Continuous Improvement and Innovation

teachSTEM actively seeks new and better ways to protect children and improve transparency in data use:

- Exploring privacy-by-design principles in new digital tools.
- Engaging youth and families in co-design of data-informed projects.
- Partnering with technology and policy leaders to remain at the forefront of ethical, inclusive innovation.