

PRIVACY & DATA PROTECTION POLICY

Last reviewed: 17th February 2026

1. Who we are

Theiyā Arts is a South Asian and Global Majority–led arts organisation working across Scotland through four strands:

- Dance Collective
- Theiyā Arts School
- In the Community
- Connect

We are a data controller for the personal information we collect and use in relation to our programmes, staff, freelancers, volunteers, participants and audiences.

Contact for data protection queries

Email: hello@theiyaarts.org

If you have questions about this Policy or how we use your data, please contact us using the details above.

2. Purpose of this Policy

This Policy explains:

- what personal data we collect and why;
- how we use and store personal data;
- our lawful bases for processing under UK data protection law (UK GDPR and Data Protection Act 2018);
- your rights;
- how we handle data relating to children and young people, including images and social media.

This Policy applies to all personal data processed by Theiyā Arts in connection with our work.

3. Our Data Protection Principles

We will:

- process personal data lawfully, fairly and transparently;
- collect data only for specified, explicit and legitimate purposes;
- collect only the data we need (data minimisation);
- keep data accurate and up to date where necessary;
- keep data no longer than necessary (storage limitation);
- keep data secure and confidential (integrity and confidentiality);
- be accountable and able to demonstrate compliance.

These principles apply to data on adults, children and young people.

4. What Data We Collect and Why

We may collect the following types of data, depending on how you engage with us.

4.1 Participants, Learners and Parents/Carers

- Contact details (name, address, email, phone).
- Emergency contact details.
- Age and date of birth (particularly for children and young people).
- Access, health or support needs (e.g. disabilities, allergies, access riders).
- Demographic information provided voluntarily (e.g. ethnicity, gender, postcode) to support our equality, diversity and inclusion monitoring.
- Registration and attendance records.
- Payment and booking details (e.g. tickets, class fees).
- Permissions for photographs, video and social media.
- Feedback, evaluation forms and creative responses.

We collect this to:

- run classes, workshops, performances and events safely;
- communicate with you about sessions, changes and opportunities;
- meet our safeguarding, health and safety and insurance obligations;
- understand who we are reaching and improve inclusion;
- report anonymised data to funders and partners.

4.2 Staff, Freelancers and Volunteers

- Contact details and emergency contacts.
- Application and recruitment information (CV, references, interview notes).
- Right to work documentation.
- Contract and payment details (bank details, fees, salaries).
- Disclosure / PVG membership and safeguarding information where required.
- Training and CPD records.
- Performance, supervision and HR-related records (kept minimal and relevant).

We collect this to:

- recruit and contract people fairly and legally;
- pay fees and salaries;
- meet safeguarding and legal obligations;
- support supervision, learning and wellbeing.

4.3 Audiences, Mailing List and Website Users

- Names and contact details for our mailing lists and bookings.
- Ticketing and event booking information.
- Communication preferences.
- Basic analytics data (e.g. page views, website traffic patterns) – usually anonymised or pseudonymised.

We collect this to:

- send you information you've asked to receive;
- manage events, tickets and attendance;
- improve our communications and website.

5. Lawful Bases for Processing

We use the following lawful bases under UK GDPR:

- **Contract** – to deliver what we've agreed with you (e.g. a class booking, employment or freelance contract).
- **Legal obligation** – to meet our legal duties (e.g. safeguarding records, financial records, health and safety reporting).

- **Legitimate interests** – where processing is necessary for our legitimate organisational interests and these are not overridden by your rights and interests (e.g. general programme administration, evaluation, internal reporting).
- **Consent** – for specific things where we need your clear permission, such as:
 - adding you to a marketing mailing list;
 - using your or your child’s image for publicity or social media (especially for children and young people);
 - collecting certain special category data (e.g. ethnicity data for EDI monitoring).

Where we rely on **consent**, you can withdraw it at any time by contacting us.

For **special category data** (e.g. health, ethnicity), we process this only where necessary and with an appropriate condition (such as explicit consent or substantial public interest in equality monitoring, where applicable).

6. How We Store and Protect Data

We take appropriate technical and organisational measures to keep personal data secure, including:

- password-protected devices and accounts;
- restricted access to systems and folders (only those who need to see data can access it);
- regular updates of software and security settings;
- secure cloud storage providers with appropriate protections;
- locked cabinets or secure storage for any paper records;
- minimising use of portable media (e.g. USB sticks) and using encryption where needed.

We will:

- keep data only as long as necessary for the purpose it was collected;
- regularly review retention periods and delete or anonymise data that is no longer needed;
- minimise duplication of personal data across systems.

7. Data Sharing

We will not sell your data.

We may share personal data with:

- venue partners or co-delivery organisations when needed for safe delivery (e.g. access lists, emergency information), under clear agreements about confidentiality and data protection;
- funders and partners, in **anonymised or aggregated form** (e.g. numbers, patterns, equality monitoring statistics);
- statutory bodies (e.g. local authority, police, social work) where required for safeguarding, legal obligations or to protect vital interests (e.g. risk of serious harm);
- payroll providers, accountants and banks for processing payments;
- IT and ticketing providers that process data on our behalf under appropriate data processing agreements.

Where we work with third-party processors, we ensure they:

- only process data on our instructions;
- keep it secure;
- comply with data protection law.

We will not transfer your data outside the UK/EEA unless appropriate safeguards are in place.

8. Data Retention

We keep personal data for no longer than is necessary for the purpose it was collected.

Indicative retention periods:

- Participant and class records: normally up to 3 years after last engagement, unless safeguarding or legal reasons require longer.
- Safeguarding records: in line with safeguarding guidance and legal requirements (often longer than other records).
- Employment and freelance records: in line with employment and tax requirements (often 6 years after relationship ends).
- Financial records: usually 6 years after the end of the financial year.
- Mailing list details: until you unsubscribe or ask us to delete your details.

Retention periods may change in line with updated guidance; we will review them periodically.

9. Children, Young People and Social Media

We work extensively with children and young people through Theiyā Arts School, In the Community and certain Connect projects. We are especially careful with their data and images.

9.1 Consent and Legal Basis

- For children and young people, we will seek **parent/carer consent** for:
 - collecting and storing personal data beyond what is strictly necessary for safety and administration;
 - using images or video of children/young people for publicity, social media or online platforms.
- Young people may also be invited to give their own views and assent, in addition to parental consent.
- Where we use social media or online platforms, we will consider terms of use and age limits.

9.2 Images, Video and Publicity

We will:

- Use **specific, informed consent forms** for photography, audio and video recording, clearly explaining:
 - what will be captured;
 - where it may be used (e.g. website, social media, print);
 - how long we may use it;
 - that consent can be withdrawn for future use (though not always for materials already printed or widely distributed).
- Provide options to:
 - give consent for internal documentation only;
 - opt out of all photo/video use;
 - allow group images but not named images, etc.
- Clearly identify children/young people who should not be photographed or shared online and brief staff and photographers accordingly.
- Avoid sharing personal details (e.g. full name, contact information, school) alongside images of children/young people, unless absolutely necessary and with explicit consent.
- Never tag children or young people's personal accounts from Theiyā Arts official accounts.

9.3 Social Media Safety

We will:

- Use organisational accounts, not personal accounts, for official communication.
- Avoid one-to-one direct messaging with children and young people from organisational accounts except where necessary and agreed as part of a safeguarding-compliant arrangement (e.g. group messages with parents/guardians copied in).
- Encourage use of parent/carer email or phone contacts rather than direct contact details of children under 18.
- Respond quickly to any concerns raised about online bullying, inappropriate comments or unwanted contact in relation to our programmes, in line with our Safeguarding Policy.
- Avoid posting content that could reveal sensitive information (e.g. exact locations at specific times with children present, unless needed and risk-assessed).

9.4 Data Minimisation for Children and Young People

We will collect only the information we need for:

- safe participation (e.g. medical/allergy information, emergency contacts);
- safeguarding and legal obligations;
- anonymised evaluation and reporting.

We will not collect unnecessary sensitive data about children's lives, identities or families, and we will treat any such information with particular care.

10. Your Rights

Under data protection law, you may have the following rights:

- **Right to be informed** – to know how your data is being used.
- **Right of access** – to ask for a copy of the personal data we hold about you.
- **Right to rectification** – to ask us to correct inaccurate or incomplete data.
- **Right to erasure** – to ask us to delete certain data where we have no good reason to keep it.
- **Right to restrict processing** – to ask us to limit how we use your data in certain circumstances.
- **Right to data portability** – to receive data you have provided in a portable format, where applicable.

- **Right to object** – to object to processing based on legitimate interests or direct marketing.
- **Rights in relation to automated decision-making and profiling** – which we do not routinely use.

To exercise these rights, contact us at [insert email]. We may need to confirm your identity before acting on a request.

If you are unhappy with how we handle your data, please contact us first so we can try to resolve the issue. You also have the right to complain to the Information Commissioner's Office (ICO) in the UK.

11. Data Breaches

A data breach is any incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Theiyā Arts will:

- take all suspected or confirmed breaches seriously;
- contain and investigate the incident;
- assess the risk to individuals;
- notify the ICO and, where appropriate, affected individuals where the breach is likely to result in a risk to rights and freedoms;
- record breaches and review how to prevent recurrence.

12. Training and Accountability

We will:

- provide basic data protection awareness training for staff and regular freelancers, including how to handle personal data securely;
- include key data protection responsibilities in induction;
- ensure those handling more sensitive data (e.g. safeguarding, HR, evaluation) receive additional guidance;
- integrate data protection considerations into our feminist MEL processes and policy reviews.

Responsibility for data protection rests with the Board and core team, with a named lead for data protection nominated within the organisation.

13. Changes to This Policy

We may update this Policy from time to time to reflect changes in law, guidance or our practices.

We will:

- post the updated Policy on our website;
- highlight significant changes to staff, freelancers, participants and partners where appropriate.