Streets Ahead Collective CIC

Data Protection (UK GDPR) Policy
Approved by the Board on: [insert date]
Version: 1.0
Next Review: [insert date, 12 months later]

1) Who we are and scope

Streets Ahead Collective CIC ("we", "us") is the data controller for personal data processed in our programmes, community activities, training, retail/gallery activities, volunteering and fundraising. This policy applies to all personal data we process in the UK under the UK GDPR and Data Protection Act 2018.

- **Registered address:** Rock Paper Scissors, 22–24 Stour Street, Canterbury, Kent, CT1 2NZ
- **Data Protection Lead (DPL):** Elizabeth (Liz) Wellstead, liz@rockpaperscissors.co.uk
- **Note:** As a small CIC we are not required to appoint a statutory DPO; we instead appoint a Data Protection Lead who performs similar duties appropriate to our scale.
- ICO registration: [**ICO registration number once confirmed**]

2) What data we process

We process identity, contact, demographic, safeguarding, education, image, health, payment, and HR/contractor data.

3) Why we process data

Delivering programmes, workshops and community activities for people of all ages, monitoring inclusion and impact, managing volunteers and partners, communications, and compliance.

4) Our lawful bases

Contract, Legal Obligation, Legitimate Interests, Consent. Special category data only under explicit consent or safeguarding condition.

5) Children and young people

We work with people of all ages and backgrounds. Where we collect data from children or young people, we comply fully with the ICO's Children's Code (Age-Appropriate Design Code) to ensure their privacy and safety online.

6) How we collect and share data

Collected via Typeform, Google Drive, email, and events. DPAs in place. Marketing follows PECR rules.

7) Security

Access control, encryption, training for all staff, contractors, and volunteers; secure disposal; and device protection.

8) Your rights

Access, rectification, erasure, restriction, objection, portability, consent withdrawal. Respond within one month.

9) Retention and deletion

Data retained only as long as necessary per Annex A.

10) Breach response

Incident log maintained. Notify ICO within 72 hours if risk to rights/freedoms.

11) DPIAs

Conducted for high-risk processing or children's services.

12) Governance, training, and review

Annual review by board, induction and refresher training for all staff, contractors, and volunteers.

Annex A — Retention & Deletion Schedule

Record type	Example content	Retention period	Rationale
Financial & accounting	Invoices, receipts, payments	6 years + current FY	Statutory and tax compliance
Contracts & grants	Supplier and funder agreements	6 years after end	Limitation Act compliance
Bookings & event admin	Attendance lists, forms	2 years after event	Query handling and reporting
Marketing lists	Emails, preferences	Until opt-out + 2 years	Audit and opt-out suppression
Safeguarding	Incident and child protection logs	Until age 25 or 8 years after last contact	Safeguarding best practice
Accident/incident	Accident forms	3 years (or until age 21 for minors)	Personal injury limitation period
HR and Contractor Records	Freelance contact details, payment info, right-to-work checks	3 years after engagement ends	Freelancer reference and legal compliance
Volunteers/ freelancers	Agreements, applications	3 years after engagement	Reference and audit trail
CCTV/venue footage	Video	30 days	Security and proportionality

Photographs/films	Media with consent	Until consent withdrawn or 5 years	Review cycle and usage renewal

Annex B — Processor Register

Processor	**Purpose**	**GDPR compliance mechanism / notes**
Google Workspace	Email, storage, documents	DPA in place; encryption; UK SCCs/IDTA
Typeform	Online forms and surveys	DPA/SCCs; encrypted; EEA/UK hosting
Shopify	E-commerce, payment data, customer accounts	GDPR-compliant platform; DPA and SCCs included

Annex C — Subject Access Requests (SAR) Quick Guide

Verify identity; log the request; respond within one month (extendable to three). Redact third-party data; no fee unless manifestly unfounded or excessive.

Annex D — Data Breach Response (First 72 Hours)

Contain > Assess risk > Notify ICO (if necessary within 72 hours) > Notify individuals if high risk > Document and learn.

Annex E — Internal SAR & Breach Playbook

This one-page guide provides staff with immediate steps if a data access request or breach occurs.

Step / Hour	Action	Responsible
SAR-1	Verify requester identity and log date	All staff / DPL
SAR-2	Acknowledge request within 3 days	DPL
SAR-3	Collect and review data, redact third-party info	DPL / CEO
SAR-4	Respond within one month (extendable to 3)	DPL
Breach 0–4h	Contain breach, preserve evidence, inform DPL	All staff
Breach 4–24h	Assess risk to individuals and systems	DPL
Breach ≤72h	Notify ICO if risk to rights/freedoms	DPL / CEO
Post-72h	Notify affected individuals and document	DPL / Board

Addendum – HR and Contractor Records

Streets Ahead Collective CIC currently engages freelancers and contractors rather than employees.

We retain records necessary to manage those engagements (e.g., contracts, contact details, payment information, and right-to-work checks) for three years after the end of engagement, unless a longer retention period is legally required.

Should Streets Ahead Collective employ staff in future, this policy and the retention schedule will automatically apply to employee records (e.g., personnel, payroll, training, and references).

Board Approval

Approved by the Board of Streets Ahead Collective CIC on:

_____

Signed (Chair): _____

Signed (CEO): _____