Data Protection Policy

Sidney Cooper Arts Trust

Table of contents:

1. Purpose

Sidney Cooper Arts Trust ("the Charity") is committed to protecting personal data and ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy sets out how personal data is collected, used, stored, and safeguarded.

2. Scope

This policy applies to:

- Trustees
- Employees
- Volunteers
- Contractors and partners who process personal data on behalf of the Charity

3. Principles

The Charity will comply with the seven principles of UK GDPR:

1. Lawfulness, fairness, transparency – data processed legally and openly.
2. Purpose limitation – data collected for specified, legitimate purposes only.
3. Data minimisation – only data necessary for the purpose is collected.
4. Accuracy – data kept accurate and up to date.
5. Storage limitation – data retained only as long as necessary.
6. Integrity and confidentiality – data kept secure.
7. Accountability – trustees responsible for demonstrating compliance.

4. Roles & Responsibilities

- Trustees: act as Data Controllers, ensuring compliance.
- Staff & Volunteers: must follow this policy and report breaches.
- Data Protection Lead: appointed by trustees to oversee compliance, training, and breach reporting.

5. Data Rights

Individuals have the right to:

- Access their personal data.
- Request correction or deletion.
- Restrict or object to processing.
- Data portability (where applicable).

Requests must be responded to within one month.

6. Security Measures

- Password protection and encryption for electronic records.
- Restricted access to personal data on a “need-to-know” basis.
- Secure storage for paper records.
- Regular backups and anti-virus protection.

7. Data Retention

- Personal data retained only as long as necessary for its purpose.
- Standard retention period: six years for financial records (HMRC requirement).
- Other data reviewed annually and securely destroyed when no longer needed.

8. Data Breaches

- Any suspected breach must be reported immediately to the Data Protection Lead.
- Serious breaches reported to the Information Commissioner’s Office (ICO) within 72 hours.
- Trustees will investigate and take remedial action.

9. Training

- All staff, trustees, and volunteers receive data protection induction.

- Refresher training provided at least every two years.

10. Review

This policy will be reviewed annually by trustees and updated in line with changes to legislation or ICO guidance.