GDPR & Data Privacy Policy

Policy Approved on: 20/11/2025

Policy Review Date: 20/11/2026

Introduction

This policy sets out how Creative at HeART CIC complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 in relation to all staff, directors, freelance practitioners, and volunteers.

Creative at HeART CIC is committed to protecting the privacy and personal data of all individuals we engage with, including children, young people, families, staff, and supporters. The purpose of this policy is to ensure that personal information is handled lawfully, securely, and transparently, in line with our community values, safeguarding responsibilities, and legal duties as a data controller.

This policy applies to all personal data held by Creative at HeART CIC, whether stored electronically, on paper, or through creative outputs (e.g., artwork produced during sessions).

Responsibility

• The Board of Directors holds overall accountability for data protection compliance within Creative at HeART CIC.
• The CEO acts as the organisation's Data Protection Lead (Data Controller), responsible for day-to-day implementation, oversight, and ensuring adherence to this policy.
• All staff, practitioners, and volunteers must comply with this policy and undertake relevant data protection training.
• Failure to comply may result in disciplinary action or, in serious cases, referral to regulatory authorities.

Any individual who believes that Creative at HeART CIC has not complied with this policy should contact the CEO (Data Controller) as soon as possible.

Key Terminology

In line with the UK GDPR, Creative at HeART CIC uses the following terms:

• Personal Data – Information that identifies, or could identify, a living individual (e.g., name, address, or personal circumstances).

• Special Category Data – Sensitive data requiring additional protection (e.g., health, ethnicity, religion, or sexual orientation).

• Data Subject – The individual whose personal data is being processed (e.g., a child, parent, or staff member).

• Processing – Any action involving personal data, such as collection, storage, sharing, or deletion.

• Data Controller – The organisation that determines how and why personal data is processed.

• Data Processor – A third party processing data on behalf of the controller (e.g., payroll provider or cloud storage provider).

Data Protection Principles

Creative at HeART CIC upholds the following key principles of data protection. All personal data must be:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Retained no longer than necessary.
6. Processed securely, maintaining integrity and confidentiality.
7. Not transferred outside the UK without adequate protection.

Lawful Bases for Processing

Creative at HeART CIC relies on one or more of the following lawful bases under UK GDPR:

• Consent (e.g., permission from parents/carers for children's participation).

• Contractual Necessity (e.g., freelance agreements).

• Legal Obligation (e.g., safeguarding reporting).

• Vital Interests (to protect life or prevent serious harm).

• Legitimate Interests (e.g., managing operations or responding to enquiries).

• Public Task (where processing supports a recognised community benefit).

Collecting and Using Personal Data

Creative at HeART CIC collects and uses personal data only for purposes that are fair, lawful, and transparent, including:

• Delivering creative and wellbeing sessions for children and families.

• Safeguarding participants and ensuring safety.

• Managing employment, volunteering, and practitioner contracts.

• Managing fundraising, partnerships, and grant administration.

• Fulfilling legal and regulatory obligations.

All individuals are informed at the point of collection about what data is collected, why it is being collected, how it will be used, stored, and shared, and their rights under the UK GDPR.

Storage, Security, and Protection of Data

Creative at HeART CIC takes all necessary steps to protect data from loss, damage, or unauthorised access:

- Digital data is stored on encrypted and password-protected systems.
- Paper records are kept in locked cabinets with restricted access.
- Only authorised staff and practitioners can access personal data.
- Children's artwork, photos, and creative materials are treated as personal data and stored securely.
- Practitioners must never leave personal data or materials unattended in public spaces or vehicles.
- Third-party processors (e.g., cloud storage providers) must sign Data Processing Agreements confirming compliance with UK GDPR.

Retention and Disposal

Creative at HeART CIC will only retain personal data for as long as necessary for operational, legal, or safeguarding purposes. After this period, data will be securely deleted, shredded, or anonymised.

A Data Retention Schedule defines how long specific types of data are held (e.g., safeguarding records, financial data, creative outputs).

Data Protection Impact Assessments (DPIAs)

DPIAs will be carried out for any new project, system, or partnership involving high-risk data processing—especially when working with children, health information, or online media. Assessments will identify and mitigate privacy risks before data collection begins.

Sharing and Disclosure of Personal Data

Personal data will only be shared on a need-to-know basis and for legitimate reasons, such as:

- With local authorities, healthcare providers, or funders for service delivery or compliance.
- With law enforcement or safeguarding partners when required by law.

Creative at HeART CIC never sells personal data or shares it for marketing purposes.

Information may be shared without consent only if required by law or to prevent significant harm.

Rights of Individuals

Under UK GDPR, individuals have the right to:

- Access personal data held about them.
- Request correction of inaccurate or incomplete data.

• Request deletion ('right to be forgotten'), where appropriate.
• Restrict or object to processing.
• Request data portability (transfer of data to another provider).
• Be informed of how their data is used.

Requests should be made in writing to the Data Protection Lead, and Creative at HeART CIC will respond within one month.

Breach of Data Privacy

Any suspected or confirmed data breach must be reported immediately to the CEO (Data Protection Lead). Examples include loss, theft, or unauthorised disclosure of personal information.

Serious breaches that risk individual rights will be reported to the Information Commissioner's Office (ICO) within 72 hours and, where necessary, affected individuals will be notified.

Training and Accountability

• All staff, practitioners, and volunteers must complete data protection training on induction and refresher training annually.
• Breaches of this policy or of data protection law may result in disciplinary action.
• The Board and CEO are responsible for ensuring that data protection is embedded in all operational and governance practices.

Policy Review

This policy will be reviewed annually by the CEO and Board of Directors, or earlier if required by law, regulation, or best practice.