KINETIKA
DESIGN THAT MOVES

119 Artist Studios
High House Production Park
Purfleet-on-Thames
Essex RM19 1AS

01708 202844
info@kinetika.co.uk
www.kinetika.co.uk

Data Protection Policy

Updated December 2025
Next review due December 2026

1. Introduction

Kinetika is committed to protecting the personal data of all individuals we interact with, in line with the UK GDPR and the Data Protection Act 2018. This policy sets out how we collect, use, store, and protect personal data.

2. Scope

This policy applies to personal data related to:

- Freelancers and contractors
- Community members, local artists and stakeholders
- Volunteers and trustees
- Event attendees
- Mailing list subscribers
- Customers, donors, and online purchasers

It covers all forms of personal data, including paper, electronic, and photographic data.

3. Principles of Data Protection

Kinetika commits to ensuring that personal data is:

1. Processed lawfully, fairly, and transparently
2. Collected for specified, explicit purposes
3. Adequate, relevant, and limited to what is necessary
4. Accurate and up to date
5. Stored only as long as necessary
6. Processed securely, with appropriate measures to prevent unauthorized access or disclosure

4. Lawful Basis for Processing

We process personal data on the following lawful bases:

- Consent – for photo consent, mailing lists, and marketing communications
- Contract – for freelancers, volunteers, and contractual arrangements
- Legal obligation – for financial transactions, trustee records, and statutory compliance
- Legitimate interests – for communication and engagement with stakeholders

Special category data (e.g., ethnicity, age, disability) is collected only when necessary and with consent.

5. Data Collection and Use

Kinetika collects and uses personal data for the following purposes:

1. Freelancer Appointments – to manage contractual arrangements and legal compliance
2. Customer Relationship Management – to maintain communication with community members, stakeholders, and local artists
3. Volunteer Management – to ensure safety, compliance, and effective communication
4. Running Events – to manage attendees, bookings, and event communications
5. Photo Consent – to obtain consent for use of identifiable images in publicity
6. Mailing Lists – to communicate with subscribers and share news and updates
7. Financial Transactions – to process sales, donations, and accounting records
8. Trustee Details – to maintain statutory and legal records

(See the Data Processing Register for full details.)

6. Data Storage and Security

- Personal data is stored on secure platforms (SharePoint, Eventbrite, MailChimp, Xero, banks, and paper files where required).
- Access is restricted to authorised personnel and protected by passwords, two-factor authentication, and controlled access.
- International transfers (e.g.MailChimp) comply with UK GDPR requirements.

Cyber Security Measures

We proactively review and maintain the security of our digital systems in line with guidance from the UK National Cyber Security Centre (NCSC) and the Digital Culture Network. These measures ensure systems remain resilient, monitored, and aligned with national best-practice cybersecurity standards.

Physical Security

- Paper records are stored securely in the office
- Access is restricted to authorised key holders
- Financial records are disposed of securely via shredding and confidential waste services

7. Data Minimisation

Kinetika ensures that personal data collected is limited to what is strictly necessary for the intended purpose.

- Data collection forms and systems are periodically reviewed to remove unnecessary fields
- Where possible, personal data is pseudonymised or anonymised
- Only required special category data is collected, with consent

8. Roles and Responsibilities

- All Freelancers, and Volunteers – follow this policy, report concerns, and complete required training
- Operations Director – oversees GDPR compliance, data breaches, and cybersecurity
- IT Support Provider (Agile Computers) – manages IT systems securely and ensures configurations comply with GDPR requirements

9. Training and Awareness

- Induction for new freelancers handling personal data – where appropriate, new starters receive GDPR and Cybersecurity training
- Refresher Training – bi-annual training sessions for all freelancers to maintain awareness and compliance

10. Rights of Individuals

Individuals have the right to:

- Access their data
- Correct inaccurate data
- Withdraw consent
- Object to certain uses
- Request deletion or restriction

Process for Handling Requests:

Requests can be made in writing by emailing info@kinetika.co.uk. These will be picked up by the Operations Director who will log and manage the request to ensure it is responded to within 1 month. In every case, the identity of the requester will be verified before actioning the request.

11. Data Sharing

Data is only shared with authorised recipients for legitimate purposes, including cloud providers, email providers, event management platforms, banks, and accounting software. All third-party processors have a Data Processing Agreements/Addendums (DPA) in place.

12. Retention

Data is retained only as long as necessary, as outlined in the Data Processing Register. After the retention period, data is securely deleted or anonymised.

13. Accountability and Review

Kinetika will:

- Maintain a Data Processing Register
- Review this policy annually or when there are changes to processing
- Keep records of consent, data breaches, and GDPR compliance measures

14. Data Breach Reporting

All staff must report any suspected data breach to the Operations Director immediately, who will investigate. Serious breaches will be reported to the ICO within 72 hours.

15. Privacy Policy

For further information on how we manage data on digital platforms, including cookies, see our Privacy Policy.

Action Plan

Core Team	Comply with GDPR training requirement	Bi-annual
	Escalate any cyber-security concerns to our IT provider, Agile Computers, for resolution	As needed and immediately
	Escalate any data collection concerns or requests for access to the Operations Director	As needed
	Make use of shared cyber security tools to protect Kinetika systems, including the NCSC Top Tips for Staff module and browser-security review tool	Ongoing
	Ensure Privacy statements are in place for each contact point of data collection	Ongoing
Operations Director	Review of Microsoft 365 Users	Quarterly
	Conduct a Cyber Security Audit to include a structured review of digital assets (website, email, and IP security), using NCSC tools and implement all high priority findings within 3 months of completion	Annual
	Arrange secure destruction of financial and special category files	Annual
	Review the Data Processing Register	Annual
	Ensure MFA is in place for critical systems – Microsoft 365, online bank logins, Xero, PayPal, Soldo, MailChimp and Eventbrite.	By March 2026
Marketing Manager	Advise team on Privacy statement requirements	Ongoing
	Review historical event data on Eventbrite and remove personal data no longer required	Twice per year
	Ensure photo consent forms are captured and securely held	Ongoing
	Review website sale information and remove personal data	Annual