

Viv'Art Movement Academy - *GDPR & Data Protection Policy*

Caring for your information with the same attention we give to every dancer

Contents

1. *Our Commitment*
2. What Information we collect
3. Why we collect personal data
4. Our Legal Basis for Processing Data
5. How We Protect Your Data
6. When We Share Data
7. How Long We Keep Data
8. Your Rights
9. Photography & Media at Viv'Art
10. Contact Us

Appendix 1: Data Breach Response Flow

Created by Alison Gee

Date: September 2026

Reviewed by Nina Monteiro

Date: September 2026

To be reviewed September 2027

1. Our Commitment to Privacy

At Viv'Art, we believe trust is part of the dance. Families share information with us so we can keep dancers safe, supported, and able to flourish — and we honour that trust with care, transparency, and respect.

We follow the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to ensure all personal data is handled responsibly and securely.

2. What Information We Collect

We collect only what is needed to deliver safe, high-quality dance education and wellbeing support.

Student Information

- Name and date of birth
- Medical and or learning needs
- Emergency contacts
- Attendance records
- Photo/video consent
- Uniform sizing information

Parent/Guardian Information

- Names and contact details
- Billing information
- Communications with Viv'Art

Staff Information

- Employment details
- Training records
- Safeguarding checks
- PL Insurance Certificates

Digital Interactions

- Website enquiry forms
- Email communications

3. Why We Collect Personal Data

We use personal data to:

- Provide safe, nurturing dance classes
- Support wellbeing and safeguarding
- Communicate clearly with families
- Manage enrolments, billing, and schedules
- Share opportunities and updates (with consent)
- Meet legal and regulatory requirements

We **never** sell or share data for commercial gain.

4. Our Legal Basis for Processing Data

Viv'Art processes data under:

- **Contract** – to deliver classes and manage enrolments
- **Consent** – for photography and marketing
- **Legal obligation** – safeguarding, HMRC requirements
- **Vital interests** – emergency medical situations
- **Legitimate interests** – running and improving our programmes

5. How We Protect Your Data

We treat your information with the same care we give to our dancers.

- Secure digital systems
- Password-protected devices
- Restricted staff access
- Encrypted storage where appropriate
- Staff training in data protection
- Safe disposal of paper records

6. When We Share Data

We only share data when necessary and appropriate:

- With staff delivering classes
- With emergency services
- With trusted third-party providers who meet GDPR standards
- When legally required (e.g., safeguarding concerns)

We do **not** share data for marketing.

7. How Long We Keep Data

We retain data only for as long as needed:

- **Student records:** enrolment period + 2 years after any departure
- **Financial records:** 6 years
- **Safeguarding records:** statutory guidance
- **Photos/videos:** only with active consent

Data is securely deleted or destroyed when no longer required.

8. Your Rights

You have the right to:

- Access your personal data
- Request corrections
- Request deletion (where legally permissible)
- Withdraw consent
- Request restriction or object to processing
- Request data portability
- Make a complaint to the ICO

Requests can be made via info@vivartmovementacademy.com

9. Photography & Media at Viv'Art

We celebrate creativity — but only with consent. Viv'Art will only capture or use images when:

- Consent has been clearly given
- The purpose is explained
- Images are used respectfully and safely
- Consent can be withdrawn at any time

10. Contact Us

Viv'Art Movement Academy Website: www.vivartmovementacademy.com

Email: info@vivartmovementacademy.com

Appendix 1: Data Breach Response Flow

A calm, clear process to protect families and staff.

1. Possible breach identified

Lost register, email error, device theft, unauthorised access.



2. Report immediately

Notify the Director



3. Contain the breach

Secure devices, change passwords, recover documents.



4. Assess the risk

What data was involved? Who may have accessed it? Is sensitive data affected? Could harm occur?



5. Notify ICO if required

If risk to individuals is high → report within **72 hours**.



6. Inform affected individuals

Provide clear, supportive communication.



7. Record the breach

Document incident, actions, and outcomes.



8. Review & improve

Update systems, training, or processes.

To be reviewed September 2027