Karate & Dance Federation

Data Protection & GDPR Policy

Policy Overview Information

Policy Title	Data Protection & GDPR
Author	Mr. Jake Byrne
Date Written	4th January 2026
Date Implemented	January 2026
Review Date	January 2027
Authorised By	Mr. Jake Byrne
Agreed By	Mr. Neil Byrne
	Miss. Alyssia Weekes

Policy Logistics

This policy is intended for the Karate & Dance Federation, which means that both companies within this umbrella organisation must adhere to the policies and procedures in place. These companies are: Central Karate Academy CIC and Midlands Dance Academy Ltd.

Umbrella organisation and governance structure

The Karate & Dance Federation operates as an umbrella organisation responsible for the strategic governance, safeguarding oversight, and operational standards applied across its constituent entities. While Central Karate Academy CIC and Midlands Dance Academy Ltd are separate legal entities with distinct legal structures, they function collectively under the Federation for the purposes of policy implementation, safeguarding assurance, quality control, and risk management.

All policies issued under the name of The Karate & Dance Federation establish a single, consistent framework of expectations, procedures, and standards that apply across both organisations. This ensures that children, families, staff, volunteers, and external partners experience the same level of protection, professionalism, and accountability regardless of which legal entity is delivering a particular activity.

Where statutory, regulatory, or reporting obligations differ due to the legal status of each entity, those obligations are met within the relevant organisation. However, the highest standard of practice set out within Federation policy will always apply. No individual, department, or entity operating within the Federation may adopt a lower standard than that required by Federation policy.

Ultimate responsibility for ensuring compliance with Federation policies sits with the Federation's senior leadership, who retain oversight of safeguarding, health and safety, professional conduct, and quality assurance across all activities delivered under the Federation name.

1. Policy statement and commitment

The Karate & Dance Federation is committed to protecting the privacy, dignity, and personal data of all individuals with whom it engages. This includes students, parents, carers, staff, volunteers, contractors, and partners.

The Federation recognises that personal data must be handled lawfully, fairly, and transparently and that effective data protection is essential to maintaining trust and safeguarding individuals, particularly children and young people.

This policy sets out how the Federation collects, processes, stores, shares, and disposes of personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope and application

This policy applies to all personal data processed by or on behalf of the Federation, regardless of format. This includes electronic records, paper files, photographs, videos, audio recordings, and online data.

The policy applies to all staff, volunteers, contractors, and anyone who has access to personal data through their role within the Federation.

All individuals are required to comply with this policy and to handle personal data responsibly and securely.

3. Definitions and types of data

Personal data refers to any information that can identify a living individual, either directly or indirectly. This includes names, contact details, dates of birth, photographs, and identification numbers.

Special category data includes more sensitive information such as health details, safeguarding records, ethnicity, and biometric data. This type of data requires a higher level of protection.

Criminal offence data, including DBS information, is processed only where lawful and strictly necessary.

4. Data protection principles

The Federation processes personal data in accordance with the core data protection principles. Personal data is processed lawfully, fairly, and transparently and is collected only for specified, explicit, and legitimate purposes.

Data is adequate, relevant, and limited to what is necessary. It is kept accurate and up to date and retained only for as long as necessary.

Appropriate technical and organisational measures are in place to ensure data is processed securely and protected against unauthorised access, loss, or damage.

5. Lawful basis for processing

The Federation identifies and documents a lawful basis for processing personal data. This may include consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests.

Where consent is relied upon, it is freely given, specific, informed, and unambiguous. Individuals have the right to withdraw consent at any time.

Special category data is processed only where an additional lawful condition applies, such as safeguarding children or fulfilling legal obligations.

6. Data collection and transparency

The Federation collects personal data directly from individuals wherever possible and provides clear information about how data will be used through privacy notices. Individuals are informed of their rights, the purpose of data collection, how long data will be retained, and who data may be shared with.

Data is not used for purposes incompatible with those originally stated without further lawful basis.

7. Data storage and security

Personal data is stored securely using appropriate physical, technical, and organisational safeguards. Electronic data is protected through password controls, encryption, and restricted access.

Paper records are stored securely and accessed only by authorised individuals. Portable devices and removable media are used with caution and protected against loss or theft.

Staff are responsible for ensuring that personal data is not left unattended or accessible to unauthorised individuals.

8. Data sharing and third parties

Personal data is shared only where lawful, necessary, and proportionate. Data sharing may occur with schools, local authorities, safeguarding agencies, insurers, or service providers.

Where data is shared with third parties, appropriate data sharing agreements or contracts are in place to ensure compliance with data protection requirements.

Personal data is never sold or shared for marketing purposes without explicit consent.

9. Individual rights

Individuals have rights in relation to their personal data, including the right to access, rectify, erase, restrict processing, object to processing, and data portability.

Requests to exercise data protection rights are handled promptly and in accordance with legal timescales. Identity is verified before responding to requests.

Children's data is handled with particular care, and parental rights are respected where appropriate.

10. Data breaches and incident management

A data breach occurs where personal data is lost, accessed, disclosed, or altered unlawfully. All data breaches or suspected breaches must be reported immediately to senior leadership.

The Federation has procedures in place for investigating, managing, and reporting data breaches. Where required, breaches are reported to the Information Commissioner's Office (ICO) and affected individuals.

Learning from data breaches is used to strengthen data protection practices.

11. Retention and disposal of data

Personal data is retained only for as long as necessary for the purpose for which it was collected and in line with legal and organisational requirements.

When data is no longer required, it is disposed of securely, whether through shredding of paper records or secure deletion of electronic data.

Retention schedules are maintained and reviewed regularly.

12. Training, awareness and accountability

Staff and volunteers receive data protection training as part of their induction and ongoing development. Awareness of data protection responsibilities is reinforced regularly.

Senior leadership ensures accountability for data protection compliance and oversees policy implementation.

13. Monitoring and review

Data protection practices are monitored regularly through audits, reviews, and incident analysis.

This policy is reviewed annually and updated to reflect legislative change, regulatory guidance, or organisational development.

14. Policy breaches

Failure to comply with this policy may result in disciplinary action, termination of engagement, and/or legal consequences.