Information Governance and Data Protection Manual

Contents

1. Introduction and Governance Framework

1.1 Purpose and Organisational Role

The Aikido Alliance (the Alliance) is a volunteer-led Sport Governing Body (SGB). Its primary function is to provide central governance, policy frameworks, and regulatory oversight to its autonomous member associations. The Alliance acts as the overarching body for the practice and development of Aikido within the United Kingdom, ensuring that member associations adhere to unified standards of safety and administration.

1.2 Governance-Only Statement

The Aikido Alliance is strictly a **Governance-Only** organisation. It does not engage in the physical delivery of aikido or related activities. All physical delivery and membership management is the responsibility of the autonomous member associations and their respective clubs.

1.3 Board Responsibilities for Data Oversight

The Alliance Officers hold collective responsibility for Information Governance. As the Data Controller, the appointed Officers ensure the Alliance meets its legal obligations under UK data protection law. Responsibilities include:

- Approving all data protection and information security policies.
- Maintaining strategic oversight of the Coaching Register and safeguarding suitability decisions.
- Ensuring the security and integrity of the Alliance's digital infrastructure.
- Promoting a culture of "Privacy by Design" within the volunteer network.
- Ensuring compliance with all relevant legislation

1.4 Key Appointments

- **Governance Lead:** Responsible for strategic oversight of governance arrangements and safeguarding leadership.
- **Safeguarding Lead:** This role makes final suitability decisions regarding individuals entering the Coaching Register based on DBS outcomes and reports serious governance incidents to the Board.
- **Data Protection Lead:** Responsible for day-to-day compliance, maintaining the Coaching Register, handling Data Subject Access Requests (DSARs), managing the data breach protocol, and serving as the primary liaison for the Information Commissioner's Office (ICO).
- **Coaching Lead:** Responsible for developing and delivering coach education and CPD
- **Insurance Officer:** Responsible for liaising with and appointing insurance brokers to ensure appropriate cover is in place for affiliated Associations, their club, coaches and members

  NB Multiple roles may be undertaken by the same person

2. Scope and Legislative Compliance

2.1 Scope

This manual is mandatory for all Board members, volunteers and contractors acting on behalf of the Aikido Alliance. It applies to all personal data processed by the Alliance, primarily stored within the Google Workspace environment.

2.2 Governing Legislation

The Alliance complies with the following:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.

2.3 Data Limitation Statement

Important: the Aikido Alliance does not process special category health data (Article 9 UK GDPR). As a governance-only body, data processing is limited to personal data (Article 6) and criminal offence/DBS suitability data (Article 10) necessary for SGB administration.

3. Key Data Protection Principles

All Alliance personnel must manage data according to the following principles:

1. **Lawfulness, Fairness, and Transparency:** Process data only for legitimate SGB purposes and ensure the Privacy Policy is accessible to all registrants.
2. **Purpose Limitation:** Data collected for the Coaching Register must never be used for third-party marketing or unrelated administrative tasks.
3. **Data Minimisation:** Only record the minimum data required to verify an instructor (e.g., name, qualification status, and DBS renewal date).
4. **Accuracy:** The Data Protection Lead must conduct annual audits of the Coaching Register to ensure details are current.
5. **Storage Limitation:** Adhere strictly to the retention schedule; data must be permanently deleted once its retention period expires.
6. **Integrity and Confidentiality:** All Alliance data must be stored in the approved Google Workspace environment to prevent unauthorised access.
7. **Accountability:** The Alliance must maintain a Record of Processing Activities (ROPA) and breach logs to demonstrate compliance.

4. Categories of Data and Lawful Basis

The Alliance processes data under the following justifications:

Data Category	Examples	Lawful Basis (Art. 6)	Justification
Association Lead Contact Details	Name, official email, telephone number.	Legitimate Interests	Necessary for the SGB to communicate governance updates to member bodies.
Coaching/Instructor Registration	Qualification records, training dates, name.	Performance of a Contract*	Required to register individuals as qualified instructors within the SGB framework.
Insurance Records	Proof of cover, names of insured officials.	Legal Obligation	Necessary to ensure the SGB and its members meet mandatory liability requirements.
DBS Suitability Decisions	Suitability status (Cleared/Not Cleared), renewal date.	Legal Obligation	Required to fulfil safeguarding duties and verify eligibility for regulated activity.

Note: Where a direct contract between the Coach and the Alliance does not exist, processing is justified under **Legitimate Interests, as verifying qualifications is essential for the safety and integrity of the sport.*

4.1 Article 10 Compliance (Criminal Offence Data)

The Alliance complies with Article 10 by processing "Criminal Offence Data" only under the official authority of the Disclosure and Barring Service (DBS). **The Alliance does NOT retain copies of DBS certificates.** Records are limited to "suitability decisions" (the outcome of the check) and the "renewal dates."

5. Individual Rights and Data Subject Access Requests (DSARs)

Individuals have rights to access, rectify, or erase their data. The Data Protection Lead handles all requests.

5.1 DSAR Response Procedure

1. **Identity Verification:** The Lead must verify the requester's identity. In accordance with **Data Minimisation**, identity documents (e.g., passport) should only be requested if the individual is not already personally known to the Lead. Any copy ID provided must be destroyed immediately after verification.
2. **Acknowledge:** Confirm receipt within 5 working days.
3. **Collate:** Gather all files, including Google Drive documents and emails related to the individual.
4. **Redact:** Ensure no third-party personal data is disclosed. On rare occasions redaction may be required to meet legal obligations.
5. **Response:** Provide the data securely and free of charge within **30 days**.

6. Information Security (Google Workspace)

To ensure the Alliance (as the Controller) maintains ownership and oversight of its information, the following security protocols are mandatory:

- **Ownership and Storage:** All Alliance documents, registers, and files must be stored in **Google Shared Drives**, not personal "My Drive" folders. This ensures that data remains the property of the Alliance if a volunteer leaves.
- **Access Control:** Access to sensitive folders (e.g., DBS Suitability) must be restricted to the Safeguarding, Governance and Data Protection Leads.
- **Data Transfer:** All Alliance business and data transfers must be conducted exclusively through the **official Alliance organisational account** (aikidoallianceuk@gmail.com). The use of **individual personal email accounts** (e.g., a volunteer's private Gmail, Hotmail, or Outlook account) for processing, receiving, or storing Alliance data is **strictly prohibited** to ensure organisational accountability and security.
- **Device Security:** Any device used to access Alliance accounts must be encrypted, password-protected, and have an automatic screen lock enabled.
- **Secure Sharing:** Document sharing must be restricted to **"Specific People"**. The "Anyone with the link" setting is prohibited for any document containing personal data.

7. Data Breach Management

A personal data breach is a security incident leading to the accidental or unlawful destruction, loss, or unauthorised disclosure of personal data.

7.1 72-Hour Response Protocol

1. **Contain:** Revoke access permissions or recall the email immediately.
2. **Report:** Notify the Data Protection Lead within 24 hours.
3. **Assess:** Determine the risk to the individuals affected.
4. **Notify:** If the breach poses a risk to rights and freedoms, the Data Protection Lead must notify the ICO within **72 hours**.

7.2 Severity Matrix

Severity	Description (examples)	Action
Low	Internal misdirected email to a trusted Board member. No sensitive data involved.	Record in Internal Breach Register.
Medium	Accidental disclosure of the Association Lead contact list to the wider membership.	Investigate; notify affected leads; record in register.
High	Unauthorised disclosure of DBS suitability data; Loss of administrative access to Google Workspace (e.g., MFA lockout of all admin accounts).	**Immediate Board escalation.** Subjec to further risk assessment, notify ICO within 72 hours; notify affected individuals.

8. Data Retention Schedule

Records must be permanently deleted in accordance with the following schedule:

Record Type	Retention Period
Association Lead/Membership Records	Duration of membership + 3 years.
Coach/Instructor Registration Records	Duration of registration + 6 years.
DBS Suitability Records	Duration of active role + 1 year.
Financial Records	**6 years from the end of the financial year** in which the transaction occurred.
Website Enquiries	6 months.

Governance Appendices Pack: Data Protection Manual

This document provides the consolidated and renumbered appendices for the Aikido Alliance governance manual. These Appendices are designed to ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, specifically tailored for the administration of a National Sports Governing Body.

Appendix A: Record of Processing Activities (ROPA)

The following table constitutes the official Record of Processing Activities for the Aikido Alliance.

Processing Activity	Purpose	Data Categories	Lawful Basis (Article 6)	Recipients
Membership Administration	Managing membership applications, renewals, and communications.	Name, postal address, email, telephone, membership information.	**Article 6(1)(b)**: Performance of a Contract	Internal staff, insurance providers.
Coaching/Instructor Registration	Maintaining records of qualified instructors and coaches.	Name, qualification and training records, insurance-related records.	**Article 6(1)(b)**: Performance of a Contract; **Article 6(1)(f)**: Legitimate Interests	Internal staff, insurance brokers, training providers.
Association Lead Management	Maintaining contact lists for association, club, or organisation leads.	Name, club/organisation details, email, telephone number.	**Article 6(1)(f)**: Legitimate Interests	Internal staff, other association leads.
DBS Verification	Verifying eligibility for roles involving children or adults at risk.	Name, **Date of Birth**, DBS status, and renewal dates.	**Article 6(1)(c)**: Compliance with a Legal Obligation	Safeguarding Lead, regulatory authorities.
Safeguarding	Protecting children and adults at risk; fulfilling safety and legal obligations.	Name, safeguarding training records, eligibility information.	**Article 6(1)(c)**: Compliance with a Legal Obligation	Safeguarding agencies, local authorities, legal counsel.

Appendix B: Data Protection Impact Assessment (DPIA) Template

This template should be copied and used to identify and minimise privacy risks for new projects, such as the introduction of new database systems or volunteer management processes.

1. Project Description

- [Insert Project Title]
- Description: [Provide a clear summary of the project or change in practice.]
- Purpose: [Explain why this activity is being undertaken and the intended outcomes.]

2. Necessity and Proportionality

- Why is personal data required? [Explanation]
- How does this comply with data minimisation? [Explain how you are using the minimum data necessary.]

3. Risk Identification

- Unauthorised access: [Identify risks regarding access to coach or volunteer records.]
- Data loss: [Identify risks regarding the loss of digital or paper records.]
- Volunteer DBS Data: Have specific risks related to processing and storing volunteer DBS status data and criminal record history been considered?

4. Mitigation Measures

- Technical Controls: [e.g., Multi-Factor Authentication, encryption.]
- Organisational Controls: [e.g., Training, restricted access permissions.]

5. Sign-off

- Data Protection Lead Approval: [Name/Date]

Completed reports will be stored within the Google Workspace

Appendix C: Information Asset Register (IAR)

This register maps the information assets held by the Aikido Alliance, including digital and physical records.

Asset Name	Asset Owner	Format	Location	Access Level
Coaching Database	Coaching Lead	Electronic	Google Workspace (Sheets/Drive)	Restricted to officials
DBS Status Log	Safeguarding Lead	Electronic	Alliance Gmail (Restricted Folder)	Safeguarding Lead only
Association Lead List	Data Protection Lead	Electronic	Google Contacts / Workspace	Restricted to officials
Insurance Documents	Insurance Officer	Electronic	Google Drive	Premium information restricted to officials. Insurance cover details – public access via the website
Physical DBS Notes	Safeguarding Lead	Paper / Electronic	Locked Filing Cabinet (Secure Office) / scan to Drive	Safeguarding Lead only
Financial Records	Governance Lead	Electronic	Google Workspace / Gmail	Restricted to Officers/DPO
Safeguarding Records	Safeguarding Lead	Paper / Electronic	Locked Filing Cabinet (Secure Office) / scan to Drive	Safeguarding Lead only

Appendix D: Data Subject Access Request (DSAR) Form

Members, coaches, or volunteers may use this form to request a copy of the personal data held by the Aikido Alliance.

SECTION 1: PERSONAL DETAILS

- **Full Name:** _____
- **Role (Member/Coach/Volunteer):** _____
- **Email Address:** _____
- **Telephone Number:** _____

SECTION 2: DATA REQUESTED

- **Description of Information:** [Please provide details of the specific data you are requesting, including relevant dates where possible.]

SECTION 3: IDENTITY VERIFICATION To protect your privacy, we must verify your identity before releasing data. Please provide a copy of a valid ID (e.g., Driving Licence or Passport).

- **Note:** Identity documents are used solely for verification and are **destroyed immediately** after your identity is confirmed.

Signature: _____ **Date:** _____

INTERNAL USE ONLY

- **Date Request Received:** _____
- **Statutory Response Deadline (1 Month):** _____
- **ID Verified by:** _____
- **Date ID Destroyed:** _____

Appendix E: Data Breach Reporting Form

This internal form must be completed by staff or volunteers as soon as a suspected data breach is discovered.

1. **Date of Discovery:** [Insert Date and Time]
2. **Name of Person Reporting:** [Insert Name]
3. **Nature of the Incident:** (e.g., Misdirected email from Alliance Gmail, unauthorised access to Google Drive, lost device).
4. **Description of Data Involved:** (e.g., Names and email addresses of coaches, DBS renewal dates).
5. **Initial Containment Actions:** [Describe what you did to stop the breach, e.g., "Recalled misdirected email", "Changed Google password"].
6. **Potential Impact:** [Describe the likely consequences for the individuals affected].

Appendix F: Data Breach Register

The Data Protection Lead will use this table to track all reported incidents. *Example shown below*

The Breach Register is not considered to be public information and the live register will be maintained outside of this document

Ref No.	Incident Description	Risk Level	Action Taken	ICO Notification Status
AA-001	*Email containing coaching qualification details sent to incorrect recipient via Alliance Gmail.*	*Medium*	*Email recalled; recipient contacted to confirm deletion; instructor notified.*	*Not Required*

Appendix G: Information Security Standards

All Aikido Alliance officials must adhere to these mandatory standards to ensure the security of organisational data.

- **Official Account Directive:** All official Aikido Alliance business **MUST** be conducted via the official @gmail.com or Google Workspace account. The use of personal email accounts for sensitive Alliance business is strictly **PROHIBITED**.
- **Password Strength:** All accounts must be protected by strong, unique passwords.
- **Role-Based Access:** Google Drive folder permissions must be restricted to only those individuals who require access for their specific role. Access levels must be reviewed annually.
- **Mobile Device Security:** Any mobile device used to access the Alliance Gmail account **MUST** be password/PIN protected and have remote-wipe capabilities enabled.
- **Physical Asset Management:** Any physical records (e.g., DBS verification notes, paper membership forms) **MUST** be stored in locked filing cabinets within secure premises. Sensitive documents **MUST NEVER** be left unattended in public spaces or at Aikido clubs.
- **Back-up Drives:** Must be held securely within office premises (or equivalent)

Appendix H: Staff and Volunteer Confidentiality Agreement

CONFIDENTIALITY AGREEMENT

As a staff member or volunteer for the Aikido Alliance, I acknowledge that I may have access to sensitive information, including instructor qualification records and safeguarding data.

1. **Duty of Confidentiality:** I agree to maintain the strict confidentiality of all personal data and safeguarding information I access during my role. I will not disclose such information to unauthorised parties.
2. **Security Standards:** I acknowledge that I have read and will comply with the Information Security Standards (Appendix G), including the management of physical and digital records.
3. **Official Tools:** I agree to use only the official Aikido Alliance digital tools and @gmail.com accounts for Alliance business.
4. **Breach Reporting:** I agree to report any suspected data breach immediately to the Data Protection Lead using the official reporting form.

Signature **Date:** **Print Name:**

Copies of completed forms will be held in the Google Workspace

Appendix I: Data Retention Schedule

The Aikido Alliance retains personal data only for as long as necessary to fulfil the purposes for which it was collected.

Record Category	**Retention Period**	**Final Action**
Membership Records	Duration of membership + 3 years	Secure Deletion / Shredding
Financial Records	6 years	Secure Deletion / Shredding
Coaching/Instructor Registration	Duration of registration + 6 years	Secure Deletion / Shredding
DBS Status Records	Duration of active role + 1 year	Secure Deletion / Shredding
Safeguarding Records	As necessary for legal and regulatory obligations	**Review for permanent archiving**