



# DATA PROTECTION POLICY

*Version 1.0 – 10th August 2018*

<http://www.bab.org.uk>

*Copyright © The British Aikido Board 2010. All Rights reserved*

## **List of Contents**

**Preface**

- 1 Introduction**
- 2 Responsibilities**
- 3 Data Security**
- 4 Retention of Documentation**
- 5 Encryption**

## **Preface**

This document details the policy by which the British Aikido Board (BAB) controls information: both personal information and information forwarded for the public domain.

The BAB is committed to the correct and legal handling of data and as required by the constitution all BAB must comply with this policy.

To this end, the BAB has put into place procedure, guidelines and toolkits for all its Member Associations detailing their legal responsibilities. These guidelines are available by download from the “downloads” section of the BAB web site: [www.bab.org.uk](http://www.bab.org.uk)

The BAB is registered with the Information Commissioner’s Office (ICO)

## 1 Introduction

### 1.1 Aim of this Policy

The British Aikido Board (BAB) needs to collect, keep and use information on Member Associations, and their individual members who come into contact with the BAB, in order to carry out its day to day operations, meet its objectives, and to comply with legal obligations. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards in place as listed in this policy.

The aim of this policy is to ensure that everyone handling personal data is fully aware of these requirements and acts in accordance with the data protection principals.

This policy covers BAB Board Members, BAB Officers, Volunteers, Member Associations and Association individual members who, for the purposes of this policy, shall be considered as 'Data Subjects'.

### 1.2 Definitions

In line with the principles of the EU General Data Protection Regulation, the BAB will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specific and lawful purpose;
- Be adequate, relevant but not excessive;
- Be accurate and kept up to date;
- Not be held longer than necessary;
- Be processed in accordance with the rights of data subjects;
- Be subject to appropriate security measures;
- Not to be transferred outside the European Economic Area (EEA).

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The GDPR suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e:

- **Accountability:** Those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the GDPR's data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.

- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data;
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

### 1.3 Types of Information Processed

The BAB processes the following personal information:

- **Member Associations:** Contact information including: Name, Address Postcode, Email, Telephone, Mobile Phone and Login Password.
- **Individual Members:** Name, Address, Postcode includes Latitude & Longitude for mapping purposes, Date of Birth, Email, Telephone Number, Mobile Phone Number, login password, Club membership, Coaching Qualifications, Grade, DBS Information, Insurance / Membership Status and any related data.
- Personal information can be kept in the following forms: Online Database, Local PC Spread Sheet, and Paper.
- Groups of people within the organisation who will process personal information are appointed BAB Officers, including Executive Committee and BAB Appointed Officers.

### 1.4 Responsibilities

Under GDPR, overall responsibility for personal data in a not for profit organisation rests with BAB.

The BAB delegates tasks to a Data Controller who within the BAB is called the Data Protection Officer. The Data Protection Officer is responsible for:

- Understanding and communicating obligations under the GDPR;
- Identifying potential problem areas or risks;
- Producing clear and effective procedures;
- Notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.
- Obtaining any required consents

All Members and Officers of the British Aikido Board who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy may result in:

- Penalty enforcement against the BAB or BAB Officers;
- Penalty enforcement against the Member Associations, its Clubs and their individual members;
- Reputational damage to the British Aikido Board and the Member Association
- Damage, discomfort or anguish of individuals.

## 1.5 Policy Implementation

To meet our responsibilities under GDPR:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised;
- Ensure the correct Notices have been advised at the data collection point.

The BAB will ensure that:

- Everyone managing and handling personal information is provided with support and guidance to allow them to do so. Where appropriate, training will be made available;
- Anyone wanting to make enquiries about handling personal information, whether an individual member, Member Association, or Officer, knows what to do;
- Any disclosure of personal data will be in line with our procedures;
- Queries about handling personal information will be dealt with swiftly and politely

## 1.6 Training

Training and awareness raising about the GDPR and how it is followed in the BAB will take the following forms:

- On assuming a position that involves gathering or handling personal information.
- All Officers of the BAB have been distributed with a copy of this document. Should additional training be required, the BAB Webmaster or Data Protection Officer is available to give advice.
- Gathering and Checking Information

Before personal information is collected, we will consider:

- What details are necessary for the purpose
- How long the BAB is likely to need this information

## 2 Responsibility

2.1 The BAB will inform people whose information is gathered about the following:

- Why the information is being gathered
- What the information will be used for
- Who will have access to their information (including third parties)

2.2 The BAB will take the following measures to ensure that personal information kept is accurate:

- Consideration needs to be given to whether personal sensitive information is held, as it should only be used for the exact purpose for which permission was granted.
- Emails will be sent to the Member Associations and individual members when information concerning them is updated.
- Member Associations and individual members have the opportunity to login into the online system to check and edit their own information, Online deletion will only be allowed by the MA and IM when the Legal Requirement to hold the data has passed otherwise they will need to contact the Data Protection Officer to assist.

### **3 Data Security**

This document details the life cycle of data held within the BAB.

#### **3.1 Physical Security (Paper based systems)**

All reasonable physical security measures are to be taken to ensure the physical security of the data commensurate with the sensitivity of the data.

Paper files are to be locked away in filing cabinets when not in use.

Where possible Cross-Cut Shredding is the preferred method of disposal of paper records

#### **3.2 Electronic Security**

All electronic data held on computers is held securely: namely in a reasonably protected location on a computer system with reasonable up-to-date anti-virus, anti-spam and anti-malware software installed.

It is expected that any computer system housing BAB information is protected by a firewall. Most Broadband routers include this feature as well as the computers operating systems.

Local backups are to be taken on a regular basis. Individual officers are required to ensure there is a valid backup of data taken before any paperwork used to input to a computer system is destroyed.

All backups are treated with the same level of secure handling as paper data: namely locked away and disposed of securely (shredded using suitable software). All local backups are held for the prescribed period of time.

Local backups should be password protected, the password must be supplied to the BAB Webmaster. In this way, should there need to be a requirement to access an Officer's backups, and the Officer is absent, it can be achieved.

Online backups may be used as long as the security of the file location is confirmed by the service provider. Account details and passwords must be copied to the BAB Webmaster.

All computer systems housing BAB Data require a strong password. All passwords should be a minimum of 8 characters and should include upper case, lower case and numeric characters. It is recommended that one of the first 6 characters of the password is a “special character” (such as !”£\$%^&\*()~@’#{[]+\_-=").

## **4 Retention of Documents**

Paper copies of the forms are kept for **17 years**, after which they are destroyed.

Electronic data is held for 17 years either online or backup in the main BAB system, or archived to the BAB database archive area.

Where there has been a data breach the information will be held indefinitely.

## **5 Encryption**

The BAB online systems will, where necessary, encrypt sensitive data