Policy 20 : Data Protection Policy and Guidelines

20.0 Data Protection Policy, Rules and Procedures

20.1 Definitions

Data Controller:	A controller determines the purposes and means of processing personal data; in this case the owner of the information is the British Aikido Association.
Data Processors:	A processor is responsible for processing personal data on behalf of a controller, in this case it will be club officers who are responsible for memberships
Data Protection Officer:	A DPO is responsible for monitoring internal compliance.
Data Retention Policy:	This is the British Aikido Associations guidance on the collection, storage, security, retention and destruction of information
Data Protection Rules:	Are the British Aikido Associations' rules and regulations through Working Practices related to GDPR regulations
Fair Processing Notice:	Provides clear statement on how the Association collects and uses personal data
Privacy Notice:	Provides overarching outline of the Associations data protection rules, regulations and procedures.
Data Subject:	Is the individual whom particular personal data is about e.g. registered member or affiliate of the association.
Personal Data:	Anything that might lead to the identification of a person: name, address, date of birth, characteristics, photography or correspondence.
Processing:	Operation, which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Consent	Must be freely given, specific and an unambiguous indication of the subjects wishes. It must be recorded and available to an audit. A person must be 13years old in order to record their consent.
Personal Data Breach	A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unoutherised disclosure, sale or access to any processed data. Data subjects affected by the data breach must be informed of the breach within 72 hours. Breaches must also be reported to the ICO within 72 hours.
Encryption	The act of encoding all the information beyond a password or code
Password Protection	The act of locking a device or electronic document. The information is only readable beyond the password.

Pseudonymisation The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

20.2 Principles

a. Fair and lawful process
b. Collected for specified, explicit and legitimate purposes
c. Adequate, relevant and limited to what is necessary
d. Accurate and, where necessary, kept up to date
e. Retained only of as long as necessary for processing
f. Processed in an appropriate manner to maintain security

20.3 Prerequisites

The British Aikido Association is required by law to comply with EU General Data Protection Regulations (GDPR) and the UK Data Protection Bill (UKDPB) and any subsequent amendments. The Association therefore needs to ensure it complies with the national guidelines in relation to data protection.

The Executive Committee of the British Aikido Association (The Association) will act as the data controller of all personal data collected by all areas of the organisation and its members, which is used for the function of the association in the pursuance of the organisation's aims and objectives. This would include any specified individuals, groups, members, clubs or affiliates covered by the association's constitution, bye-laws and working practices.

The Executive Committee (EC) of the Association appoints the Association's Data Protection Officer (DPO). The officer is responsible for apprising the EC and any other appropriate officers as indicated by the EC of any changes in requirements under the regulations and for ensuring that appropriate procedures are in place for meeting the requirements of the legislation.

The DPO will maintain

a. A fair processing notice
b. A register of suppliers who are approved to process personal data on behalf of the association
c. A register of software, which will be used for processing operations by the Association.

Elected and Appointed members, at any level should have due regard to keeping proper separation between personal data and only collect and store specific data as required by the Association to carry out its aims and objectives.

The association must only process personal data that is provided to the association by other data controllers if: -

a. There is a legal right under legislation, or
b. There is provided by the supplying data controller adequate consent under relevant legislation that the Association has the right to process the data in the pursuance of its aims and objectives.

In the event of personal data being supplied in accordance with above then it will be deemed as third party data.

20.4 Data Security

Personal data must not be processed or stored on personal computers.

Passwords for encrypted data must be transmitted via a different method than the encrypted data.

Personal data must not be processed on devices that belong to non association members, unless the processing is being undertaken by a person or company that is on the register of approved suppliers who are approved to process personal data, which will be maintained by the DPO.

Personal Data must not be processed for longer than the maximum stated in the association's data retention policy.

Personal data must only be stored on cloud based or other types of off premises systems that are specified in either

a. The software register
b. The approved supplier register

Breaches of these rules must be reported in writing to the Association's DPO within 24 hours of the breach being discovered.

Unintentional permanent loss or destruction of data must be reported in writing to the DPO within 24hours of being discovered and then with the ICO within 72 hours.

Personal data in physical form, for example, printouts and paper forms, will be processed and stored with due regard to the security of personal data.

20.5 Data Collection

Personal data will be collected in accordance with the requirements of the EU General Data Protection Regulations (GDPR) and the UK Data Protection Bill (UKDPB).

When collecting personal data

a. Via a web form, there must always be displayed a current Fair Processing Notice that is clearly legible in close proximity to the section of the form where the data is collected.
b. Via a paper form, there must always be displayed a current Fair Processing Notice that is clearly legible in close proximity to the section of the form where the data is collected.
c. Via a telephone call, it must be ensured that the person giving the data is asked to consent to the recording of the data and that they are informed of how their data will be used and how long the association will keep it.
d. By way of face-to-face conversations, it must be ensured that the person who is giving the data is handed a leaflet on which the current Fair processing Notice is clearly legible and that the person is asked to consent to the association recording the data.

Personal data about a data subject that is collected from a third party must NOT be recorded or processed unless there is specific written consent from the data subject in question

When personal data is collected all relevant consents as required by the Fair Processing Notice will be accurately recorded in the database designated in the software register.

A member of the Association who collects data in contravention of these rules will be subject to the relevant Association disciplinary procedure.

20.6 Data Use

Personal data must not be processed unless there is a lawful reason for the processing

Lawful reasons for processing: -

a. The data subject has given consent to the processing of their person data for one or more specific purposes.

b. If the data subject is an association member and processing is necessary for the performance of the contract between the data subject and the Association.

c. Processing is necessary for compliance with legal obligations to which the controller is the subject

d. Where processing is allowed by an applicable exemption stated in a schedule of the UK Data Protection Bill.

e. Where processing is allowed by other law or statute.

When relying on consent, as a reason for processing it must be ensured that any consent that was obtained prior to the implementation of these rules is adequate.

Members of the Association may only be contacted by: -

a. Unaddressed leaflets or mail

b. Addressed mail where they have specifically, voluntarily and in full knowledge of how they will be contacted, consented to be opted into receiving mail.

In addition to the contact methods above members of the Association may be contacted by mail, email, telephone, text and apps unless they have requested not to be contacted.

Individual members of the public who are not association members must not be contacted by: -

a. E-mail, unless they have specifically, voluntarily and in full knowledge of how they will be contacted, consented to be opted into receiving emails.

b. Telephone, unless they have specifically, voluntarily and in full knowledge of how they will be contacted, consented to be opted into receiving telephone calls.

c. Text, unless they have specifically, voluntarily and in full knowledge of how they will be contacted, consented to be opted into receiving text messages.

d. Social Media and Apps, unless they have specifically, voluntarily and in full knowledge of how they will be contacted, consented to be opted into receiving messages or advertisements by social media and apps.

All consents must be accurately recorded in the database designated in the software register and kept for future reference.

Withdrawal of consent must be accurately recorded in the database designated in the software register.

When relying on consent as the lawful reason for processing, that consent will only be lawful if the consent was freely given and presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easy accessible form, using clear and plain language.

Personal data may only be given to suppliers that are on the register of approved suppliers who are approved to process personal data as maintained by the Data protection Officer.

Not withstanding any of the above, personal data must not be processed if the data subject has instructed that they do not wish to have their data processed.

20.7 Data Subject Rights

Any communication from a data subject making a request or claim under any of the individuals rights such as: -

a. Right to be forgotten
b. Right to restriction of processing
c. Right to access, also known as a subject access request (SAR)
d. Any other right under the GDPR or UKDPB

Must be forwarded to the Association Data Protection Officer within 24 hours of becoming aware of the request or claim.

20.8 Fair Processing Notice Summary

Who we are

The British Aikido Association Ltd, founded in 1966, is the Lead Body for Sport Aikido in the UK, operating as a not for profit oragnisation, for the promotion and development of Aikido and related arts.

Our Fair processing Notice explains your privacy rights and how we gather, use and share **information about you, the members. If you wish to get in touch please contact or Data** protection Officer at: - **See website for details**

Your rights

You have the right to object to how we process your personal information. You also have a right to access, correct sometimes delete and restrict the personal information we use. In addition, you have the right to complain to us and to the data protection regulator.

How we gather personal information

We gather membership information given to us directly, using the membership application form. Other information is supplied through individual's attendance at gradings, competitions and coach awards and is used for the purpose of monitoring and quality standards.

How we use your personal information

We use your information to provide you with information regarding Association activities such as competitions, gradings and events. We use the information to monitor and maintain membership to ensure compliance with insurance regulations. Sometimes we need to have sensitive information such as medical details to make sure we comply with health and safety regulations

Our Services

We need some personal information to ensure that the functions of the Association can be met and inform members of key events they may wish to attend and for them to maximise the benefits of being a member.

Sharing and transferring personal information

We share specific information with our suppliers, who require this information to provide support services and benefits. We may have to share information with law enforcement and child welfare agencies if requested. We do not allow our information to be sold or used for commercial purposes.

Keeping personal information

We keep all our information securely for up to 15 years, encrypted and password protected

Your Consent

Consent is initially sought on the membership application form. Giving the Association the right to monitor membership and supply them with information. Where you have given consent you have the right to withdraw it at any time.

Our partners

We want the best for our members and sometimes we work with other agencies and companies to offer the best services available. These organisations would include e.g. insurance providers and DBS services. All partner organisations will work through the Association and should not be in direct contact with any individual member. This is to ensure the security of the information you have provided to us.

20.9 Software Register for the British Aikido Association.

Website and database - currently - www.britishaikidoassociation.co.uk

20.9 Approved Suppliers List

DBS provider – currently: **GBG, 1 Wilford Business Park, Ruddington Lane, Nottingham,NG11 7EP**

Insurance provider – currently: **Bluefin Sport, 6 St Stephens Avenue, Bristol, BS1 1YL**

20.10 Controller and Processors Contract

The contract is important so that both parties understand their responsibilities and liabilities.

Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor, which adheres to an approved code of conduct or certification scheme, may help controllers to satisfy this requirement

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

Contracts between controllers and processors:

a. ensure that they both understand their obligations, responsibilities and liabilities;
b. help them to comply with the GDPR;
c. help controllers to demonstrate their compliance with the GDPR; and
d. may increase data subjects' confidence in the handling of their personal data.

The GDPR imposes a legal obligation on both parties to formalise their working relationship.

By having a contract in place with the required terms:

a. we are ensuring that you are complying with the GDPR;
b. we are protecting the personal data of customers, staff and others
c. both parties are clear about their role in respect of the personal data that is being processed and there is evidence of this.

Contracts outlines:

a. the subject matter and duration of the processing;
b. the nature and purpose of the processing;
c. the type of personal data and categories of data subject; and
d. the obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

a. only act on the written instructions of the controller;
b. ensure that people processing the data are subject to a duty of confidence;
c. take appropriate measures to ensure the security of processing;
d. only engage sub-processors with the prior consent of the controller and under a written contract;
e. assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
f. assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
g. delete or return all personal data to the controller as requested at the end of the contract; and submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

What details about the processing must include the following details about the processing:

a. the subject matter;
b. how long it is to be carried out for;

GDPR – contracts and liabilities between controllers and processors what processing is being done:

a. its purpose;
b. the type of personal data;
c. the categories of data subjects; and
d. the obligations and rights of the data controller.
e. Therefore it needs to be very clear from the outset about the extent of the
f. processing that you are contracting out, and you can't use very general or
g. 'catch all' contract terms.

This clarity should also help to protect against the possibility of changes being made to the scope of the processing over time without taking into account any additional risks this poses to the data subjects.
Agreeing the contract or other legal act, the specific tasks and responsibilities of the processor and the risk to the rights and freedoms of the data subjects must be taken into account.

20.10 The Contract

This is a legal contract between the Controller (British Aikido Association) and approved Processors (Member club identified representative or Membership Officer). All data collected will remain the property of the individual and processed and stored by the Controller for legitimate Association activity.

All data will be securely stored on and only on the Associations database. Under no circumstances must this information be transferred, copied or stored on any other electronic device. Any printed copies must be kept safe and safely disposed of/ destroyed after each specific usage.

Sensitive personal data that is not encrypted must not be electronically transferred by any means including email.

Each Processor (one per registered club) will be provided with a password to enable them to see their club information. This password must not be transferred to any third party.

If a club changes its Membership Officer (Processor) a new password will be generated and the old one removed from service.

the subject matter of the processing

The information collected will pertain to those who wish to become or who already are members of the British Aikido Association and/or its Affiliates.
and
Information regarding member clubs and/or its Affiliates
and
Information regarding Executive Members, Fellows or Patrons of the Association and/or its Affiliates.

the nature and purpose of the processing;

This will be achieved through the completion of an application from which will be duly signed by the member (or parent or legal guardian if under 18 years of age). This application form will be available in paper and electronic formats. The information collected will be used for the purposes of the Association in the execution of informing members as to activities of the Association and its Affiliates. To ensure members insurance, provide information for DBS checks and general association management needs including validation of membership for purposes of gradings, competitions and course attendance.

the type of personal data being processed

We gather membership information given to us directly, using the membership application form. Other information is supplied through individual's attendance at gradings, competitions and coach awards and is used for the purpose of monitoring and quality standards.
Additional forms will be completed with reference to Coach Awards, Gradings and attendance registers at courses. Information regarding First Aid qualifications may also be collected and maintained.

Data on individual members including

Name, contact details (address, telephone and email) Date of Birth, Club, Grade (if any) type of membership Junior, Adult concession, health /medical details and signature.

Data on member clubs including

Dojo address, practice times and public contact details Club Coach(s)and grades, Club Contact, Club Secretary, Club Membership Officer, club website, signatures and social media details.

Consent to opt into the Association processing personal data and Acknowledgement of the Fair Processing Notice.

Consent to opt into receiving promotional information related to British Aikido Association, Worldwide Sports Aikido Federation and member club events including competitions and seminars.

Consent to opt into photography from competitions and events to be used on the associations website and promotional flyers.

No other information is to be collected, processed or retained.

The categories of the data subjects

The subjects of data processing include current and past members and those wishing to apply for member under any of the categories of membership as outlined on the Associations application form. This form must be completed by all new members with opt in clearly identified and acknowledged by the member or parent.

20.11 Details of the duration of the processing

Processed information will be retained by the Association for a total of 15 years with a staged reduction in the amount of data retained.

Schedule of processing

Stage One data removed after 15 years would include contact details including address, telephone and email. DOB, medical information and signature

Stage Two after 20 years any information processed regarding disciplinary procedures, insurance claims or legal documentation.

Stage Three retained in historical records include name grade, coaching qualification, competition records.

The Association retain the right to publish competition results and grading results as part of the ongoing development of the history archive of the Association

the obligations and the rights of the controller

Obligations :-

a. To maintain data in a safe and secure environment
b. To provide clear and relevant information through the Fair Processing Notice.
c. To provide opt in clauses
d. To provide individual subjects the right to access their information and the right to destroy.

Rights: -

f. The data subject has given consent to the processing of their person data for one or more specific purposes including the administration of the Associations activities.

g. If the data subject is an association member and processing is necessary for the performance of the contract between the data subject and the Association.
h. Processing is necessary for compliance with legal obligations to which the controller is the subject
i. Where processing is allowed by an applicable exemption stated in a schedule of the UK Data Protection Bill.
j. Where processing is allowed by other law or statute.

20.12 The processor acts on the documented instructions of the controller

The processor is a club member who is responsible for the collection and administration of subject data. They collect Association data under the direct responsibility of the Association "Controller" and can be subject to audit by the Associations DPO.

The processor may not hold data in any other form either electronic or paper, other than for short-term usage for specific events such as a grading, competition or collection of membership applications. Once processed onto the central database all other data must be destroyed.

Access to the central database will be through a dedicated password and will allow access only to individual club membership data.

To upgrade information on the central database the amended information must be forwarded to the Association membership Officer / Appointed Controller.

20.13 The processor

The processor must delete or return the personal data at the end of the provision of services or on cessation of role any communication from a data subject making a request or claim under any of the individuals including: -

e. Right to be forgotten
f. Right to restriction of processing
g. Right to access, also known as a subject access request
h. Any other right under the GDPR or UKDPB

Appropriate technical and organisational measures

a. All data will be maintained by the Associations appointed data "Controller"
b. All data processors will be DBS checked
c. All data will be encrypted and password protected
d. All processors will be audited
e. A DPO will be appointed to ensure data security

a right for the controller to audit the processor.

The association as Controller reserves the right, from time to time, annually, to audit the Controllers who have access to Association data. This audit will be undertaken by the Associations DPO within EU General Data Protection Regulations (GDPR) and the UK Data Protection Bill (UKDPB) regulations.